National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

NAVAL CYBER WARFARE: ARE CYBER OPERATORS NEEDED ON WARSHIPS TO DEFEND AGAINST PLATFORM CYBER ATTACKS?

LCdr J.M. Lanouette

JCSP 42

Master of Defence Studies

PCEMI 42

Maîtrise en études de la défense

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 42 – PCEMI 42
2015 – 2016

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

NAVAL CYBER WARFARE: ARE CYBER OPERATORS NEEDED ON WARSHIPS TO DEFEND AGAINST PLATFORM CYBER ATTACKS?

LCdr J.M. Lanouette

Word Count: 16 776

Compte de mots: 16 776

TABLE OF CONTENTS

ABSTRACT

Naval warships require several computer networks in order to operate at sea to fulfill its missions. These computer networks not only allow for communications between the ship and shore establishments over the defence enterprise networks, they also control the machinery that enables a ship to float and move, they ensure safe navigation, they control the weapon systems and maintain the recognized maritime and air picture for timely command and control.

As Western navies have moved to purchasing Commercial-Off-The-Shelf systems, the computer security vulnerabilities found in the commercial products have been reproduced in naval vessels. These vulnerabilities could be exploited by adversaries resulting in the disabling of ships with very little evidence to provide victims with a means of attributing the attacks to an actor. The threat of cyber attacks against naval vessels means that there is not only a requirement to secure the systems, but also to monitor the networks actively in order to detect malicious activity, respond to any cyber attacks, and to recover the systems to their full capabilities after such an attack occurs.

This paper provides an explanation of the systems required to operate a naval vessel and the security challenges of these systems. It explores several case studies of cyber events in the civilian sector and draws parallels between those attacks and the systems onboard ship. Finally, it will argue that the Royal Canadian Navy must develop a cyber operator occupation in order to successfully address the cyber threat to ship systems.

NAVAL CYBER WARFARE: ARE CYBER OPERATORS NEEDED ON WARSHIPS TO DEFEND AGAINST PLATFORM CYBER ATTACKS?

CHAPTER 1

INTRODUCTION

Ever since World War II (WWII), the computer has changed how wars are fought. The *Bombe* that permitted the allies to break the *Enigma* encoded German transmissions was an electro-mechanical computation device designed and built by Alan Turing and Harold Keen[1]. Today, networked computers allow for rapid transmission of information and increased computation power. In military applications, this advanced technology allows for the real-time display of a Common Operating Picture (COP), showing the location of known and unknown contacts, thus increasing a commander's Command and Control (C2) capabilities.[2]

Computers are at the heart of the computations required for tracking targets using radars and determining fire control solutions to engage targets with guns and missiles. Without computers, humans would be unable to process all the information required to effectively track and neutralize threats to a modern warship. The computers must synthesize all the available information and present it to the operators such that good decisions can be made in the shortest amount of time possible.

Computers are also used to monitor and control the complex systems that make up an Industrial Control System (ICS) which runs a civilian power plant, or a ship's propulsion, electrical power grid and damage control systems. These systems need continuous monitoring to ensure that they are operating within tolerance, that the machinery is supporting the demands of the plant and that corrections are being made to the operating states of the various equipment.

---

[1] B. Jack Copeland, *Colossus: The Secrets of Bletchley Park's Code-Breaking Computers* (OUP Oxford, 2006).

[2] George Crawford, "New Roles for Information Systems in Military Operations," *Air & Space Power Chronicles*, accessed April 11, 2016, http://www.iwar.org.uk/iwar/resources/airchronicles/crawford.htm.

According to several networking and security experts, hacking is the act of manipulating computers or computer networks to do the bidding of the hacker.[3] Hacking can come in the form of harmless technical experiments or can be conducted with extremely malicious intent. Much of what is shared in the news is viewed as malicious hacking activities, from minor Denial-of-Service (DOS) attacks such as Anonymous' attack on the Government of Canada over Bill C-51[4], to major cyber crime involving large thefts of data or money such as the attack on over one hundred banks across 30 countries to steal one billion dollars[5]. However, in the context of the military, cyber warfare involves two types of cyber attacks: theft of data in the form of critical information and effects through the use of cyber tools. As computer technology has evolved, so too have the abilities of hackers, both friendly and malicious. The scope of what can be achieved through the use of cyber tools has also grown immensely.

Cyber warfare involving the theft of data is effectively the act of spying, or gathering intelligence. There are several reports of such attacks on US military networks. The attack that compromised the United States (US) Department of Defense (DOD) Non-Secure Internet Protocol Router NETwork (NIPRNET) and the Secure Internet Protocol Router NETwork (SIPRNET) in 2008 was accomplished by malicious software (malware) found on a USB flash drive that was left in a DOD base parking lot by a foreign intelligence agency.[6] This attack led to

---

[3] Bradley Mitchell, "What Is Hacking?," *About.com Tech*, February 26, 2016, http://compnetworking.about.com/od/networksecurityprivacy/f/what-is-hacking.htm; Carolyn Meinel, "Computer Hacking: Where Did It Begin and How Did It Grow?," *WindowSecurity.com*, October 16, 2002, http://www.windowsecurity.com/whitepapers/harmless_hacking_book/Computer_hacking_Where_did_it_begin_and_how_did_it_grow_.html.

[4] Amy Minsky, "'Anonymous' Claims Responsibility for Cyber Attack That Shut down Government Websites | Globalnews.ca," June 17, 2015, http://globalnews.ca/news/2060036/government-of-canada-servers-suffer-cyber-attack/.

[5] "Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kaspersky Lab | SecurityWeek.Com," accessed April 4, 2016, http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab.

[6] Ellen Nakashima, "Defense Official Discloses Cyberattack," *The Washington Post*, August 25, 2010, sec. Politics, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html.

the creation of the US Cyber Command[7], one of the many steps the US has taken to provide a better cyber defence capability for its DOD networks. Most of the cyber attacks on US networks that have been reported were linked to the gathering of information, intellectual property or intelligence, such as those reported in the Mandiant Intelligence Center report *APT1: Exposing One of China's Cyber Espionage Units*.[8]

However, certain attacks were preliminary reconnaissance to build capabilities to disrupt critical infrastructure, such as power distribution plants using cyber tools[9]. These types of attacks use cyber weapons created to produce a kinetic effect. Cyber weapons could be used for state on state warfare by crippling a nation's infrastructure. Similarly, these same attacks could be used against naval warships to prevent them from completing missions they've given by their governments. For a warship to sail, the ship's captain must have confidence that the ship's systems will function as designed when needed. Should malware find its way onto one of the many networks that control machinery, weapons or command and control (C2) systems, the reliability of these systems would be severely compromised.

As a warship is highly dependent on its computer systems to operate safely at sea and to conduct its business of maritime defence, weaknesses it these same systems could be exploited to prevent a ship from sailing or from collecting valid reconnaissance data. This weakness could be exploited by hackers who are well funded and resourced. Therefore, modern navies must be prepared to defend a warship from a cyber attack and ensure that ships' systems maintain their availability and reliability while at sea. Although it is unlikely that navies will ever conduct offensive cyber activities from sea – there is no advantage to be gained by doing so as bandwidth

---

[7] Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Cyber Conflict Studies Association, 2013).

[8] Mandiant Intelligence Center, "APT1: Exposing One of China's Cyber Espionage Units" (Mandiant, 2013).

[9] Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, April 9, 2009, sec. Tech, http://www.wsj.com/articles/SB123914805204099085.

limitations exist for most ships – there is a need for hackers on board ships to defend them from intrusions and subversion.

This paper will argue that the Royal Canadian Navy (RCN) must prepare itself for the potential that cyber weapons will be used against its vessels by attacking the confidentiality, availability and integrity of its systems. This cannot be done by simply purchasing the latest anti-malware product from the many vendors that market their solutions as the magic device or software that will keep networks safe, such as Bromium, FireEye and Cisco.[10] While many of these vendors' products provide excellent security, the security landscape continually changes and requires cyber operators to remain vigilant and to keep the tools relevant against modern threats.[11] This paper will provide the background information required to understand why warships are at risk of being targeted using cyber weapons and why the RCN should take steps to prepare itself to defend a warship from a cyber attack while at sea. This paper will not discuss the tactical employment of cyber operators on warships, nor detail the technical methods and techniques to defend computer networks. However, in order to understand what the threats are to warships, certain technical aspects of cyber attacks and how to counter them will be described. This paper will also not describe any precise threats or vulnerabilities that systems in RCN ships have in order to remain unclassified, however there have been vulnerability assessments conducted on some of the systems on RCN ships that are available in the classified realm.

The first chapter will discuss the state of the art of systems found on today's warships. These systems include the mechanical and marine systems that provide power, propulsion and ancillary capabilities for the ship, the systems that allow the ship to safely navigate and the

[10] "Bromium Endpoint Protection & Endpoint Security," accessed April 11, 2016, https://www.bromium.com/; "Endpoint Security | Detect and Block Endpoint Attacks," *FireEye*, accessed April 11, 2016, https://www.fireeye.com/products/hx-endpoint-security-products.html; "Network Security Products and Solutions," *Cisco*, accessed April 11, 2016, http://www.cisco.com/c/en/us/products/security/index.html.

[11] Kristin E. Heckman et al., "Denial and Deception in Cyber Defense," *Computer* 48, no. 4 (2015): 36.

combat systems that enable the ship to be a warship. It will reveal that these systems, while sharing significant characteristics with traditional corporate network, are significantly unique and require their own security controls and specialists to ensure their security and monitor their performance. The second chapter will present a survey of cyber events, from the early intelligence gathering of the KGB to the latest in attacks on critical infrastructure that resulted in kinetic damage. It will highlight the increasing complexities of existing malware, the level of sophistication possible by state sponsored hackers as well as the increasing trend of impact that cyber attacks are having on critical infrastructure. The third chapter will link the cyber events from chapter two to the technology presented in chapter one, presenting the argument that the RCN must develop cyber operators to defend Canadian warships from cyber attacks. It will discuss the types of people required to do the job, the academic and technical abilities that will need to be imparted on them, and the command structure that they would fit into on the ship. It will also argue that the RCN must not rely solely on technology to accomplish its missions, and that returning to certain manual methods may be necessary for areas of naval professionalship that connect be protected by naval cyber operators. Finally, this paper will provide a summary of the content and recommendations for future study into developing naval cyber operators.

.

CHAPTER 2

COMPUTERS IN THE MODERN WARSHIP

Introduction

Warships in the days of sail relied solely on manual labour and wind power to conduct the business of the world's navies. The naval vessels of the World Wars were significantly better equipped mechanically with large boilers being fired with coal, massive guns manually trained by gunners, however navigation was still being conducted by hand on paper charts and shooting stars at night to obtain a fix on the ship's position. The modern warship has evolved significantly in the late 20th century and especially in the last 15 years. They are now powered by large gas turbines, diesel engines or nuclear reactors. Their weapons systems are dealing with missile engagements that are occurring at speeds exceeding the speed of sound. Navigation systems are highly reliant on technology with the adoption of the Global Positioning System (GPS) and electronic charts as the main means to navigate a ship.

The computer networks that comprise the many different systems on warships are different from traditional computer networks. While traditional computer networks and military embedded systems share many similarities, such as the use of desktop computers, operating systems such as Windows or Linux and applications to permit the exchange of data, data on military operating networks is critical and highly time sensitive, often requiring the use of real-time systems rather than general purpose operating systems.[12] They also have specialized devices that communicate between control consoles and the physical devices that are not found in traditional networks.

[12] Steve Furr, "What Is Real Time and Why Do I Need It?" *Military Embedded Systems Resource Guide*, 2002, 12, http://pdf.cloud.opensystemsmedia.com/mil-embedded.com/QNX.May05.pdf.

This chapter will argue that the interconnectedness of modern computerised control technologies that are necessary to make a modern warship float, move and fight all require detailed and highly specialised knowledge to keep the systems operational and protect them from contemporary cyber threats. It will also reveal that these systems have unique intricacies that require specialized knowledge to maintain, operate and secure them effectively. The first section of this chapter will explain the control systems used to monitor and control a ship's power generation, propulsion and damage control systems. The second section of this chapter will discuss the navigation systems used on board modern warship's. The third section will present the modern Combat Management System (CMS) that integrates the ship's sensors, weapons, navigation and countermeasure systems. The fourth section will detail the security challenges associated with the three categories of systems that are presented in this chapter.

Industrial Control Systems (ICS)

Modern warships have sophisticated marine engineering plants comprised of engines and auxiliary machinery in order to operate. The main engines provide the propulsion for the ship, along with gearboxes and shaft lines that help transfer the energy from the engine to the propellers. Auxiliary engines provide power generation for a ship to be able to power all its systems onboard, be it lighting, radars, or guns. Auxiliary machinery, such as pumps are used for sea and fresh water cooling systems, fuel systems and fluid level management in ballast, fuel and water tanks. All of these systems require constant monitoring to ensure that they are operating correctly in order to guarantee that the ship can float and move. Computers allow for the automation of many of the control functions for these systems. This section of the chapter will discuss the architecture of ICSs, the protocols used and their criticality.

ICSs are significantly different from commercial or corporate computer networks in different ways. Typical computer networks provide a means of exchanging information between users over a Local Area Network (LAN) which in turn is connected to a Wide Area Network (WAN) such as the internet. ICSs on the other hand exist to control physical equipment and thus have multiple layers of connections where devices are connected to controllers, controllers are then connected together, and these are then interfaced with a Master Station which provides centralized management and monitoring through a Human Machine Interface (HMI). This allows humans to monitor and control the systems on the network.[13] These differences mean that an ICS has different Quality of Service (QoS) criteria than home or office networks, such as having deterministic behaviour[14] and real-time data transfer.[15][16] It also means that the result from computer failures on an ICS can cause significant physical damage to equipment and could lead to the loss of life.

The term SCADA is often used interchangeably with ICS. It stands for Supervisory Control and Data Acquisition. These systems, as well as Distributed Control Systems (DCS) are used in many civilian distribution centres for water, natural gas and electrical power grids.[17] They provide centralized monitoring of the control systems and allow for remote control of circuit breakers, valves, pumps, engines and other field devices. The main differences between

---

[13] B. Galloway and G. P. Hancke, "Introduction to Industrial Control Networks," *IEEE Communications Surveys Tutorials* 15, no. 2 (Second 2013): 861, doi:10.1109/SURV.2012.071812.00124.

[14] Deterministic behaviour is defined as an algorithm that given the same input will always exhibit the same behaviour, as opposed to non-deterministic where an algorithm given the same input over different runs will exhibit different behaviour.

[15] Galloway and Hancke, "Introduction to Industrial Control Networks," 861.

[16] Quality of Service (QoS) is a term used in computer networking that identifies the important criteria in providing the necessary service of the consumer, be it data transfer speed, latency or delay in transmission from source to destination, jitter (variation in latency), etc. In ICS, the different QoS means that the inherent design of the software must be completely different than that of a corporate network in order to achieve deterministic behaviour and real-time data transfers.

[17] Ernie Hayden GICSP, Michael Assante, and Tim Conway, "An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity," 2014, 17, https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf.

SCADA systems and DCSs are that SCADA systems event driven, are spread over large geographic areas and are suited to multiple independent systems while DCSs are process driven, used in small geographic areas and are suited to large, integrated systems.[18] The remote control aspect of the ICS permits operators and/or automated commands to adjust the behaviour of any of the field devices within the distribution system itself. The devices that provide an interface between the SCADA system and the field devices are called Remote Terminal Units (RTU). These are comprised of "the communication interface, a central logic controller, and an input/output system with analog inputs, digital inputs, control digital outputs and sometimes analog control outputs."[19] The RTUs provide the interface between the computer network and the mechanical systems, relaying current system state to the supervisory controller and passing digital commands to the mechanical devices to change their state to provide the desired services. The mechanical devices are connected to Programmable Logic Controllers (PLC) that are responsible for taking the digital commands and converting them to analog responses to actuate the changes in the machinery, and conversely, receiving the analog data from sensors and converting them to digital signals to be returned to the Master Station[20]. The HMI is the computer application that gives the operator access to all the information on the status of the network and the various field devices. It allows the operator to change the state of any of the devices or to set the conditions for the system to generate its own responses to set conditions.

Historically, ICSs used fieldbus protocols to provide the communications stream between the control and the instrumentation devices. These protocols were created to replace two-wire signaling techniques that required each device to have its own dedicated serial port to the

[18] Galloway and Hancke, "Introduction to Industrial Control Networks," 864.
[19] GICSP, Assante, and Conway, "An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity," 17.
[20] Galloway and Hancke, "Introduction to Industrial Control Networks," 863.

controllers. The fieldbus protocols allowed for a LAN type architecture to be used instead of direct serial connections between individual devices. This spurred several different proprietary and open source protocols.[21] An International Electrical and Electronics Engineering (IEEE) Power and Energy Society (PES) committee was formed in the late 1980s to examine the problems with the proliferation of fieldbus protocols. It examined over 120 protocols against industry requirements and selected two protocols moving forward.[22] Initially, these were completely separate from the protocols used in Ethernet based networks, due to the different QoS requirements of industrial systems. Given the proliferation of Ethernet computer networking devices in home and offices, there are significant economies of scale that can be achieved by using similar interfaces in ICSs.[23] As Ethernet technologies have improved, new protocols have been developed to allow ICS to function over Ethernet while maintaining their ability to meet their QoS requirements.[24]

ICS, DCS and SCADA systems are connected to critical infrastructure, such as natural gas, water purification and distribution services, electrical power generation and distribution grids and public transportation systems in civilian applications and that they are vital to the everyday life of the average citizen of Western countries.[25] These same systems are also prevalent in military applications, notably in warships. As these systems are so essential to everyday life, the severity of a failure in an ICS could lead to equipment damage, environmental disasters and potentially the loss of life.[26] Two examples in recent history illustrate this fact.

---

[21] Ibid., 865–66.

[22] GICSP, Assante, and Conway, "An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity," 19.

[23] Galloway and Hancke, "Introduction to Industrial Control Networks," 867.

[24] Ibid., 869.

[25] Richard G. Bensing, "An Assessment of Vulnerabilities for Ship-Based Control Systems" (Monterey, California. Naval Postgraduate School, 2009), 31–32, http://calhoun.nps.edu/handle/10945/4646.

[26] Galloway and Hancke, "Introduction to Industrial Control Networks," 861.

First, the well publicized Stuxnet attack caused the physical destruction of nuclear centrifuges in an Iranian Nuclear refinement facility in January 2010.[27] A second example of an attack on a control system was the cyber attack on a German steel foundry in December 2014 which caused physical damage to a blast furnace.[28] These two examples reveal the reality of the outcomes of cyber attacks on control systems that manipulate physical devices. They will be further explored in Chapter 2.

Warships can be viewed as miniature cities, requiring their own power generation, water distribution and sewage handling, in addition to propulsion, ballast control and damage control. Because these systems are essential for warships to conduct their missions, their security is an extremely important consideration for designers and operators.[29]

Thus far, this paper has presented the technical complexities of a typical ICS and discussed the importance of securing these systems. It should be noted that securing these systems as well as monitoring and ensuring their continued security requires specialized skills, even greater than traditional network security specialists, owing to the differences between an ICS and a traditional corporate network. Another type of computer network and associated devices that is equally important for a ship to be safe at sea is the navigation suite.

Navigation Systems

As important as the ICS and mechanical equipment is to allow a ship to move and stay afloat, so too is the ability for the ship's captain to safely navigate. There are several systems onboard modern ships that form an integrated navigation system. This section will briefly cover

[27] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon | WIRED," accessed November 6, 2015, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[28] "Cyberattack on German Steel Plant Caused Significant Damage: Report | SecurityWeek.Com," accessed April 6, 2016, http://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report.

[29] Bensing, "An Assessment of Vulnerabilities for Ship-Based Control Systems," 35.

the purpose of each part of navigation equipment that makes up a typical ship's navigation system and the impact to a ship should any of these be compromised.

The United Nations (UN) International Maritime Organization (IMO) outlines essential navigation equipment in the International Convention for the Safety of Life at Sea (SOLAS). In this convention, it mandates that ships shall have the necessary navigating equipment to ensure safety at sea. The specific requirements increase with increasing ship tonnage. For typical naval warships which range between 2,000 tons for corvettes to 95,000 tons for aircraft carriers, the types of navigation equipment that are mandated by SOLAS include a means to determine ship's heading using a gyro-compass, nautical charts (usually in the form of an electronic chart display and information system or ECDIS), a Global Positioning Satellite (GPS) receiver, depth recorder, speed through water recorders, navigation radars, electronic plotting aids, an Automatic Identification System (AIS), and an automatic feed of ship's heading and speed to the navigation radar, the AIS and the plotting aid.[30] While naval warships are not actually subject to SOLAS[31], it is common practice to make every effort to comply with the SOLAS regulations. All RCN warships are equipped with the above mentioned navigation equipment.

In addition, warships require precise ship attitude data in order to accurately aim their weapons. The gyro-compasses on warships are typically fed the ship's heading from inertial navigation systems which also provide pitch, roll and yaw data to the ship's ICS and CMS. All of the ship's navigation systems are connected together via a navigation network, sometimes referred to as an Integrated Bridge System (IBS)[32] or as is the case for the *Halifax* class frigate,

[30] International Maritime Organization (IMO), "International Convention for the Safety of Life at Sea," November 1, 1974, 274–77.

[31] Ibid., 14.

[32] "Navigation Integrated Bridge System – Marine Systems - L-3 MAPPS," accessed April 6, 2016, http://www.mapps.l-3com.com/navigation-integrated-Bridge-System.html.

the Navigation Data Distribution System (NDDS). These systems act as a hub or switch for the network, ensuring the right data is sent to the systems that require it.

Most modern warships use ring laser gyro inertial navigation systems (INS) in order to determine the ship's attitude and heading. These replaced traditional gyroscopes and use lasers and mirrors to determine ship movement and acceleration in the three axes: pitch, roll and yaw. From these, they determine the changes in heading and attitude over time.[33] The INS can provide its data to other systems using synchro feeds or over Ethernet depending on how modern it is. These are then distributed through the IBS or NDDS to the various users, such as the ECDIS, the heading displays at the helm, on the bridge and in the operations room.

The ECDIS is an electronic chart display which allows a navigator to plan routes and follow them in real time, applying fixes electronically onto the chart. It serves as a means of recording a ship's navigation passages and for ensuring that the ship is following the planned course to navigate from port to port or within patrol sectors. Because it is receiving feeds from the ship's positioning systems, such as the INS and GPS, it automatically correlates the ship's position on the chart and can raise alarms should the ship be approaching navigation hazards.[34]

Navigation radars allow a ship's navigator to identify navigation hazards, such as land masses or other ships using electromagnetic (EM) waves when visibility is reduced. Most modern ship navigation radars are equipped with automatic radar plotting aids (ARPA) which fulfill the electronic plotting aid requirement in SOLAS. ARPA allows the radar to automatically create tracks based on radar contacts and displays that contact's course and speed as well as the

[33] A. D. King, "Inertial Navigation-Forty Years of Evolution," *GEC Review* 13, no. 3 (1998): 140–149.

[34] "About ECDIS | What Is ECDIS? | | ECDIS," accessed April 7, 2016, http://www.ecdis-info.com/about_ecdis.html.

closest point of approach in order to give the navigator the information required to safely navigate the ship around other vessels.

On modern vessels, an IBS integrates all these systems as well as the ship's ICS together to provide an aggregated collection of the information onto easily accessible consoles for the ship's captain and navigator.[35] This allows them to view the pertinent information they need to deal with the various navigation challenges throughout a voyage. As indicated on the L3 MAPPS website, a major vendor of IBS, these systems are built using Commercial-Off-The-Shelf (COTS) equipment.[36] This typically means that the system is built using computer components that are similar to personal computers (PC) and use commercial operating systems, such as Microsoft Windows or one of the many open source distributions of Linux, such as in the NDDS.

The automatic identification systems provide a means for vessels to identify their position, course, speed, last port of call and next port of call to nearby vessels. This information is also provided to a global shipping database via satellite communications. Dr. Marco Balduzzi, a security researcher for Trend Micro, presented significant security flaws in the AIS database as well as the AIS communications protocol itself at the Black Hat conference in Asia in March 2014. The database flaws allow any hacker with access to the AIS software, which is commercially available, to send false contact information to the server, adding ship tracks into the database for ships that aren't really there. The other flaw with the AIS protocol is that there is no verification of the content of the AIS traffic, only the format.[37] Therefore, it is possible for an

---

[35] Raunek Kantharia, "What Is Integrated Bridge System (IBS) on Ships?" *Marine Insight*, April 16, 2012, http://www.marineinsight.com/marine-navigation/what-is-integrated-bridge-system-ibs-on-ships/.

[36] "Navigation Integrated Bridge System – Marine Systems - L-3 MAPPS," 3.

[37] Format verification entails that the protocol uses error checking against a pre-determined format, ensuring that the information packet was delivered without errors. However, it does not mean that the content of the message is verified to ensure that it contains valid data. Instead of containing data about a ship's position, it could simply contain the text "Hello World" or contain database command code that could corrupt a database connected to the AIS device.

attacker to craft AIS packets that will be received by an AIS receiver and be passed on to an IBS for processing that could take advantage of vulnerabilities in the software of an IBS.[38]

Malware that could be injected into the navigation system could achieve one of two types of attacks. The first would be a Denial of Service (DOS) attack.[39] This could be purpose built to cause parts of the navigation system to stop providing its information and become unresponsive at a precise time or geolocation, leading to a significant hazard to the safe navigation of the vessel. Second, the malware could hypothetically be used to establish a covert channel for the exfiltration of information or to manipulate information within the system leading to false contact information and creating a lack of confidence in the data of the system.

Similar to a ship's ICS, a vessel's suite of navigation equipment is highly dependent on computer technology. While these two areas of shipboard equipment are common to both commercial shipping and naval vessels, there is one more category that uses similarly technologically advanced equipment that is unique to warships.

Combat Management Systems (Command and Control Systems)

While the ICS and mechanical systems provide today's ships with the means to move and float, and the navigation systems allow for ships to safely sail around the world, warships need to be able to defend and fight against the various threats that exist. In order to accomplish this in the era of supersonic missiles and extremely silent submarines, modern warships need efficient

[38] Marco Balduzzi, "AIS Exposed - Understanding Vulnerabilities & Attacks 2.0," March 2014, https://www.blackhat.com/docs/asia-14/materials/Balduzzi/Asia-14-Balduzzi-AIS-Exposed-Understanding-Vulnerabilities-And-Attacks.pdf.

[39] DOS is a category of attacks that attempt to deny a service to users. The commonly known application of this attack is against websites for companies or government agencies that hackers wish to disrupt by flooding the website with requests. Other forms of DOS attacks exist that entail causing systems to become unresponsive through endless loops or by overloading a network with a never ending stream of data, preventing other devices from communicating on that network.

detection and defence capabilities. They also require a sophisticated combat management system (CMS) in order to integrate the various systems that make up a warship's combat capabilities. A CMS will integrate a ship's many radars, sonars, early warning electronic detection systems (called electronic support measures (ESM) systems), electronic counter measures (ECM) and weapons systems. This section will discuss the use of the combat systems on a warship and the potential outcomes should these systems be compromised with malware.

A ship's sensor suite includes air and surface search radars, air and surface tracking radars, ESM early warning systems, and sonar systems. The air and surface search radars detect air and surface contacts using EM waves that are transmitted by the radar, reflect off the object and are then received by the radar system. It then processes the received waves using sophisticated computers to determine the contacts location (range, bearing and altitude), course and speed, to refine the signal to differentiate between clutter/noise and actual targets and finally, more advanced radar systems can even do target recognition.[40] Tracking radars are similar to search radars except they use slightly different detection technology to acquire and track targets for the purpose of engaging the target with either missiles or guns.[41]

ESM systems are specialized radar signal receivers that are able to identify the type of radar and thus the threat incoming to a ship. This is done by comparing the received signal's identification parameters, such as the signal frequency, pulse repetition interval, pulse width and other key identifiers with a pre-loaded electronic intelligence (ELINT) library. The library allows the ESM system to fingerprint the intercepted signals, identify the type of radar and associate it with known platforms that carry that type of radar (eg. aircraft, missiles, ships, etc), allowing an operator to determine if the emissions are of a hostile nature and whether the ship needs to take

[40] Merrill Skolnik, *Introduction to Radar Systems*, Third (McGraw-Hill Professional, 2001), 1–19.
[41] Ibid., 210.

measures to defend itself.[42] ESM systems are highly reliant on computers to be able to process the signals and compare them with the ELINT libraries.

ECM systems are a defensive measure to protect a ship from incoming missile threats. There are two types of ECM systems, those that use jamming techniques by returning falsified radar signals back to the threatening radar, called active ECM, and those that employ chaff rockets, decoys or other reflectors to distract or seduce missiles away from the ship, called passive ECM.[43] These systems can be used together when developing effective countermeasure tactics depending on the threat itself. Similar to the ESM systems, ECM systems require computers to process the threat against ECM libraries and coordinate the best countermeasure for a given threat.

Sonar systems operate much like radar systems, only they use sound waves rather than EM waves for the detection of underwater targets. The science behind sonar is quite different to that of radar, as sound travelling through water is affected significantly differently than EMc waves in air, however the basic concept of a transmitter sending a signal and listening for an echo is the same for an active sonar as for a radar system. A passive sonar simply listens to sound in the water and provides bearing information to the operator. Through significant sound processing and tactics employed by the ship, sonar operators can also determine the range and thus the location of a target underwater. Significant advances in sonar technology such as synthetic aperture sonar (SAS), which use the advanced computation power of today's micro-processors to combine acoustic pings from several sonars to provide high resolution images allow for accurate mapping of mine fields.[44] Modern sonar systems make significant use of

---

[42] Merrill Skolnik, *Radar Handbook, Third Edition*, 3rd ed. (McGraw-Hill Professional, 2008), 24.2-24.5.
[43] Ibid., 24.5.
[44] "New Sonar Developments," *Naval Technology*, February 28, 2011, http://www.naval-technology.com/features/feature111462/.

neural networks to improve their signal processing capability and thus the likelihood of underwater detection.[45] The reliance on computers is just as high in underwater technology as it is in radars.

Weapon systems on modern warships are used for both offence and defence. The armament will vary from nation to nation and from between different ship classes within a nation, however the four main categories of weapons on a warship are offensive ship-to-surface missiles such as the Harpoon Block II, defensive surface-to-air missiles such as the Evolved Sea Sparrow Missile (ESSM), naval guns and torpedoes for underwater threats. These modern weapon systems require sophisticated computers to compute the fire control solution which ensures an accurate delivery of the weapon to its target. Weapons such as the Harpoon Block II use GPS and an INS along with its built in radar system to accurately engage land targets.[46]

The CMS integrates all the sensor data from the systems mentioned above to present a complete picture of all the contacts surrounding the ship. This allows the ship's operations team to make assessments of the contacts, determine threats to the ship and prosecute the targets that do pose a threat. These contacts are usually maintained in some type of database in an application running on the CMS. A modern CMS, such as one found in the modernized *Halifax* Class ships uses a combination of COTS and Military-Off-The-Shelf (MOTS) equipment. The majority of the MOTS is for the specialized equipment that would only be used for military specific requirements, such as the air and surface search radars, fire control radars, weapon systems, sonars and the electronic warfare equipment that were discussed earlier in this section. However, the CMS itself, which integrates all the data from the various combat peripherals, is

[45] Hossein Peyvandi et al., "SONAR Systems and Underwater Signal Processing: Classic and Modern Approaches," in *Sonar Systems*, ed. Nikolai Kolev (InTech, 2011), http://www.intechopen.com/books/sonar-systems/sonar-systems-and-underwater-signal-processing-classic-and-modern-approaches.

[46] "Harpoon Block II Anti-Ship Missile," *Naval Technology*, accessed April 11, 2016, http://www.naval-technology.com/projects/harpoon-block-ii-anti-ship-missile/.

more likely to be built out of COTS equipment and software. The US Navy's most modern warship being developed – the USS *Zumwalt* – will have a CMS that will be composed of data centres using IBM blade servers (an industry standard) and the Red Hat Linux operating system.[47] This means that any vulnerabilities that exist in Linux will be exploitable on the *Zumwalt*'s system.

As the majority of these systems use some form of computing assets to perform their roles, it is possible that they have vulnerabilities that could allow a cyber attack to alter the behaviour of these systems. While in most cases these types of systems are not connected to the Internet or other outside networks, it may be possible to introduce malware through the supply chain in order to gain access to any of the systems discussed above or through social engineering by tricking maintainers to introduce the malware to the system through USB sticks. After access has been achieved, it would be possible to perform a DOS attack from within by preventing missiles from firing or by forcing the shutdown of radar systems. A much more ominous attack could cause friendly tracks within the CMS to become hostile tracks, forcing confusion in the operations room and possibly leading to friendly fire incidents.

Given the severity of the possible outcomes should shipboard systems such as an ICS, the navigation suite and the CMS and ancillary combat systems be compromised, it is clear that the security of these systems should be assessed for vulnerabilities. These vulnerabilities should be corrected as best as possible and the remaining security risks be mitigated through the use of proper monitoring tools and the employment of skilled cyber defenders. The next section of this paper will discuss the challenges involved in securing naval systems, while Chapter 3 will present the requirements (tools and personnel), for monitoring these systems.

---

[47] Sean Gallagher, "The Navy's Newest Warship Is Powered by Linux," *Ars Technica*, October 18, 2013, http://arstechnica.com/information-technology/2013/10/the-navys-newest-warship-is-powered-by-linux/.

Security Challenges of Shipboard Systems

As was previously discussed in this chapter, modern systems on naval vessels mix commercial network components with special purpose components to fulfill the three functions of a warship: float, move and fight. For instance, ECDIS applications are usually installed on computers running a variant of the Microsoft Windows operating system. The UK Admiralty ECDIS buyers guide notes that they are susceptible to virus infections.[48] Typical avenues by which malware could be introduced to an ECDIS is through updates to the electronic charts or through exchanges of route plans between navigators via USB memory sticks that have been introduced into computers that were infected. As the ECDIS are interfaced with the remainder of the navigation suite, this suggests that malware infecting an ECDIS has the potential to spread to other devices in the navigation system network and potentially to the ship's ICS or CMS.Thus, the security requirements for these networks are similar to commercial and corporate networks, however they have a greater security challenge due to type of operation requirements of these systems, such as deterministic behaviour and real-time delivery of data.[49] Some security controls may unacceptably hamper the performance, timeliness, availability capabilities of an ICS, navigation system or CMS.[50]

The differences between ICS and typical Information Technology (IT) systems described earlier in this chapter are the reason that the National Institute of Standards and Technology (NIST) have published the guidance for securing ICS: Special Publication 800-82 *Guide to Industrial Control Systems (ICS) Security)*. This document provides the necessary information to

[48] UK Hydrographic Office, "ECDIS Buyers Guide," September 2012, 22, http://www.gnsworldwide.com/sites/default/files/ecdis_buyers_guide_v2_0_19_09_12.pdf.

[49] Galloway and Hancke, "Introduction to Industrial Control Networks," 875.

[50] Keith Stouffer et al., "NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security" (National Institute of Standards and Technology, June 2015), 2–14, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

understand the differences between ICS and traditional IT systems, how to institute a risk management and assessment process specific to an ICS, and then how to develop and use an ICS security program, how to develop a secure ICS network architecture and finally, how to apply security controls in order to reduce the risk to the ICS.[51] It builds upon NIST's Special Publication 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems*, Special Publication 800-39 *Managing Information Security Risk* and Special Publication 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*. 800-37 and 800-39 describe how the US Federal Government Departments should assess and manage the security risks of their IT systems, while 800-53 lists security controls to be used to mitigate risks for specific vulnerabilities identified through applying the risk management framework of 800-37.[52] The goal of applying these security safeguards in the traditional IT systems is to "protect the confidentiality, integrity and availability of information that is processed, stored, and transmitted."[53] 800-82 highlights that while these security objectives are to be considered for ICS, the most important objective is to maintain availability.[54] This is to ensure that the ICS continuously provides the critical service for which it supports. Integrity should also be of prime concern, as incorrect data could lead to system failures that will not be reported to the operators, potentially causing physical damage. CMS provide an interesting blend of ICS and traditional IT security requirements, in that they control physical

[51] Ibid., 1–1, 1–2.

[52] Joint Task Force Transformation Initiative, "NIST Special Publication 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems" (National Institute of Standards and Technology, June 2014), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf; Joint Task Force Transformation Initiative and others, "NIST Special Publication 800-39: Managing Information Security Risk" (National Institute of Standards and Technology, March 2011), http://dl.acm.org/citation.cfm?id=2206266; Joint Task Force Transformation Initiative, "NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations" (National Institute of Standards and Technology, April 2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[53] Joint Task Force Transformation Initiative, "NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations," 1.

[54] Stouffer et al., "NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security," 6–2.

devices but also handle classified information, such as ELINT libraries, and thus have significant security requirements for confidentiality, availability and integrity.

Galloway and Hancke note that historically ICS were thought to be secure due to the level of obscurity of the devices in the system, i.e. the devices were only found in ICS and therefore would not be available to generic hackers who would try to exploit them.[55] Additionally, these devices were not connected to external networks, further reducing the attack surface. This reliance on custom electronic devices and isolated networks to make a system secure was coined "security through obscurity". However, as Jim Breithaupt and Mark Merkow, two security experts for Fortune 100 financial firms and major banks, describe in their book *Information Security: Principles and Practices*, it is impossible to forever keep the secrets of how a system is designed or how software is programmed. Once the secrets have been discovered by someone, the entire security layer provided by the obscurity disappears and the system becomes extremely vulnerable.[56] Thus, "security through obscurity" is inherently flawed and only provides a "false sense of security."[57]

Bensing recommends following the certification and accreditation policies of the DoD Information Assurance Certification and Accreditation Process (DIACAP) that have since been superseded by the risk management framework of NIST 800-37.[58] Following the risk management framework will allow for the categorization of the system based upon the three security objectives, the determination of the level of risk to the system given the threats, vulnerabilities and valuation of the system; the selection and application of security controls; the

---

[55] Galloway and Hancke, "Introduction to Industrial Control Networks," 875.

[56] M.S. Merkow and J. Breithaupt, *Information Security: Principles and Practices*, Certification/Training Series (Pearson Education, 2014), 25, https://books.google.ca/books?id=YBKpAwAAQBAJ.

[57] Ibid.

[58] Bensing, "An Assessment of Vulnerabilities for Ship-Based Control Systems," 131; Joint Task Force Transformation Initiative, "Guide for Applying the Risk Management Framework to Federal Information Systems," 1.

determination of the level of residual risk to the system once the controls have been applied; and the verification that the security controls work as intended.[59] Following this process throughout the entire life-cycle of a system, from conception to implementation and disposal would ensure secure coding practices in the software development, selection of appropriate security devices and secure configuration settings for each device on the network.

Galloway and Hancke note the importance of a layered defence for ICS, which is one of the core security principles for securing traditional IT systems.[60] They describe this layering as having separate networks at each level of service, with the core being the controllers, next the HMI and configuration layer, followed by the supervisory and data collection layer, and then a border protection layer before connection to external networks.[61] The border protection is achieved through the use of firewalls, virtual private networks (VPN) and demilitarised zones (DMZ). These will be further discussed in Chapter 3.

ICS, navigation systems and CMS share several security requirements with traditional IT systems, such as the requirement for confidentiality, availability and integrity, although less so for confidentiality of the ICS. The key to establishing a good security foundation for these systems is following a sound risk management process throughout the entire life-cycle of the system, while focusing the categorization and application of security controls within the context of the system itself, in order to ensure the system is able to fulfill its functions unimpeded by the security put in place. Achieving that balance of enough security to prevent malicious actors from causing mission failure in a system while keeping it highly functional is the main security challenge. As David Geer, a freelance technology writer wrote, putting in place too much

---

[59] Joint Task Force Transformation Initiative, "Guide for Applying the Risk Management Framework to Federal Information Systems," 18–33.

[60] Joint Task Force Transformation Initiative, "NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations," 25.

[61] Galloway and Hancke, "Introduction to Industrial Control Networks," 876.

security which impedes or interferes with the system's operation will likely cause operators to bypass the security measures put in place to protect the system.[62]

Conclusion

This chapter covered the current state of the art in automated systems onboard naval vessels used in the management of the marine systems engineering plants, the navigation of the ship and the combat systems. It highlighted the unique aspects of control systems that make up ICS and CMS, but also linked these types of systems to traditional IT systems. The roles and uses of these systems was also presented, whether this be controlling pumps and engines, displaying the ship's position on a chart, or detecting incoming threats to the ship. This was done in order to highlight the significance to the ship and its crew should one of these systems be compromised and fail to perform according to its specifications.

While navies are used to building redundancy in their systems, it was shown that a malicious actor could force an ICS, navigation suite or CMS to falsely report its data and thus the system would believe that it is operating normally and would not report a fault to an operator. This could have disastrous consequences should a mechanical system such as a gas turbine fail catastrophically or a friendly target appear as hostile in the CMS.

This chapter also covered the similarities and differences involved in implementing security measures for these systems. It was noted that there is a significant amount of publications from NIST that help system engineers to develop a risk management strategy for the securitization of the systems. While the measures discussed in the NIST publications ensure that a system is secured as best as possible, no system can ever be one hundred percent secure, and

[62] David Geer, "Security of Critical Control Systems Sparks Concern," *Computer* 39, no. 1 (January 2006): 23, doi:10.1109/MC.2006.32.

thus there is a requirement for system monitoring and defense. The methods to achieve this will be discussed in Chapter 3.

In order to fully appreciate the risks to these systems such that a proper systems security engineering process is followed in the development of these systems and that the appropriate resources are allocated to defending them, it is essential to look at what types of breaches of occurred on typical IT systems and on industrial control systems.

CHAPTER 3

REVIEW OF CYBER ATTACKS

Introduction

In order to appreciate the threats to the computer systems onboard modern naval vessels, it is important to understand what hackers are capable of doing to computers. In *Hackers: Heroes of the Computer Revolution*, Steven Levy describes the early days of hacking being limited to a select few ingenious students at the Massachusetts Institute of Technology (MIT) from the mid 1950s thru to the early 1960s who took pleasure in pushing the boundaries of computing and challenging each other to make the most efficient code with old punch card computing and later with the first transistor based computer, the TX-0.[63] This is where the hacker ethic was born: "Access to computers – and anything that might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative!"[64] This is also where the hacker mindset with respect to authority was created; hackers at MIT believed that a free exchange of information was essential, but bureaucracies from governments to corporations got in the way of an open information exchange system.[65] Thus was the birth of the modern hacker.

Today, hackers come in many varieties. Edward Skoudis describes the different types of hackers in *Counter Hack Reloaded* as falling into one of three categories. There are the white hat hackers who are security experts who conduct research and test systems for vulnerabilities in order to improve their security. There are black hat hackers who attempt to penetrate systems for malicious reasons, such as to steal money or information, hold information for ransom or for

---

[63] Steven Levy, *Hackers: Heroes of the Computer Revolution - 25th Anniversary Edition* (O'Reilly Media, 2010), 21–33, https://books.google.ca/books?id=mShXzzKtpmEC.
[64] Ibid., 40.
[65] Ibid., 41–42.

computer vandalism. Finally, there are grey hat hackers who will do legitimate penetration testing but will also attack systems for malicious reasons.[66]

The earliest attack on government networks was aimed at the US DoD, but also included defence contractors and universities. Clifford Stoll, an astronomer who became a cyber defender while working at the Lawrence Berkley Laboratory (LBL) describes the 1986 attack in an article he produced in 1988, *Stalking the Wily Hacker*, reprinted in Jason Healey's book *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* The attacker penetrated the LBL networks in order to pivot to other computers through ARPANET and MILNET[67], searching for documentation related to the Strategic Defense Initiative (SDI), or what was commonly called *Star Wars*.[68] Stoll discovered the attacker's activities because of a billing error on his computer. Along with several other computer administrators at LBL, he coordinated a counter intrusion campaign to watch the attacker's activities, determine what he was looking for and trace the attack back to the person. This involved intensive network monitoring, logging the attacker's every connection to various sites through different modems, identifying his attack patterns and methods and determining what subjects he was looking for. The attack extended to over 450 military, defence contractor and research computers. It took nearly a year of work to determine the attacker's origin and the assistance of the US Federal Bureau of Investigation (FBI) and the German equivalent, the Bundeskriminalamt (BKA) to prosecute him; he was a German working

[66] Edward Skoudis and Tom Liston, *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, 2nd ed. (Prentice Hall, 2006), 13.

[67] ARPANET and MILNET were precursors to the Internet. These networks connected military and academic networks across the US.

[68] Clifford Stoll, "Cuckoo's Egg: Stalking the Wily Hacker," in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, ed. Jason Healey (Cyber Conflict Studies Association, 2013), 89–106.

for the Union of Soviet Socialist Republics (USSR) spy agency, the Komitet Gosudarstvennoy Bezopasnosti (KGB).[69] This event marked the first documented cyber defence activity.

This chapter will outline some of the major cyber conflicts and intrusions that have occurred in the past 20 years to provide context to the threat that exists to the RCN. It will discuss three types of attacks: attacks on traditional enterprise networks, attacks on ICS of civilian facilities such as power plants, and attacks on the supply chain to introduce malware in systems before they are put into operation. The first section will discuss attacks on traditional IT networks to establish the baseline for cyber attacks that can then be leveraged in more complicated networks such as ICS. It will focus on cyber espionage and provide a concrete example in the 2008 Buckshot Yankee cyber attack. The second section will discuss attacks on ICS in order to illustrate the similarities and differences of how an ICS is exploited in comparison to traditional networks. These attacks are significantly more complicated than attacks on enterprise networks, however many aspects of attacks on traditional networks are used in parts of the attacks on ICS. The third section will present cases of cyber attacks on the supply chain which can undermine the trust in a system's devices. These three forms of cyber conflicts together should be considered in aggregate when looking at the threats to the systems on naval vessels, given that the ships have traditional networks to conduct ship and CAF administration and segregated networks for the operation of the ship. The techniques illustrated in the examples below could be used to exploit the ICS, navigation and combat systems of ships by combining them together.

[69] Ibid.

Attacks on Traditional Networks

Espionage

One of the main goals of state sponsored cyber attacks is to conduct espionage on another nation. China has been recognized as a major actor in this space. Mandiant reported that a military unit from the Peoples Liberation Army (PLA) called Unit 61398 has been engaged in cyber espionage since at least 2006, busily collecting "hundreds of terabytes of data from over 141 organizations across a diverse set of industries."[70] Mandiant called the unit Advanced Persistent Threat 1 (APT 1). The report highlights that 115 of the victim organizations were in the US, five in the UK, three each in Israel and India, two each in Canada, Switzerland, Singapore and Taiwan and finally one each in Norway, France, Belgium, Luxembourg, UAE, South Africa and Japan, illustrating that China is not focused on individual sectors of industry and is simply collecting as much information as possible in order to steal technology, produce it more cost effectively and beat these industries to market.[71]

While industrial cyber espionage in some cases leads simply to an economic advantage, in other cases it can lead to national security challenges. The Wall Street Journal reported in August of 2009 that the Lockheed Martin division responsible for the development of the F-35 Joint Strike Fighter had been infiltrated from at least 2007 well into 2008 and resulted in the exfiltration of files related to the design, performance and electronic systems of the aircraft.[72] Although China has denied that it was involved and has taken a firm stance against cyber espionage, further reporting by Defensetech.org indicates that Chinese spies hacked into secure

[70] Center, "APT1: Exposing One of China's Cyber Espionage Units," 20.
[71] Ibid., 22.
[72] Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009, sec. Tech, http://www.wsj.com/articles/SB124027491029837401.

conference calls in order to listen to classified discussions about the fighter's technologies.[73] In John Reed's article, *Did Chinese Espionage Lead to F-35 Delays?*, he highlights that the Pentagon identified that these cyber attacks led to the realization that there was no consideration for cyber security on the F-35, thus causing the necessity for the project to re-write software and redesign compromised systems of the aircraft.[74]

Mandiant's report highlights that the majority of attacks conducted by the Chinese follow a specific attack methodology, involving aggressive spear phishing[75], conducting reconnaissance of the networks, then deploying custom malware to achieve persistence[76] within the network and finally sending large amounts of compressed data back to China.[77] This highlights China's determination to acquire intellectual property. The amount of resources required to conduct the social engineering necessary to craft targeted emails, establish control on a network, and remain silent while slowly extracting the information of interest is significant. This lends credence to the term *Advanced Persistent Threat*.

While it can be argued that the systems that make a ship float, move and fight are not directly connected to networks that connect to the Internet, the cyber espionage threat presents risks to these systems from the perspective that adversaries could acquire information about the system's configuration, hardware and software in order to develop custom malware to attack

---

[73] John Reed, "Did Chinese Espionage Lead To F-35 Delays? |," accessed April 14, 2016, http://www.defensetech.org/2012/02/06/did-chinese-espionage-lead-to-f-35-delays/.

[74] Ibid.

[75] Spear phishing is the act of sending crafted emails to targeted individuals in order to have them click on a malicious link or open a compromised file, such as a Word or PDF document that has embedded malware. The emails will often appear to have been sent from a personal contact, such as a work colleague. The malware will usually establish a link back to a command and control server and establish persistence on the computer it has infected.

[76] Persistence in cyber is the ability to maintain a presence on a system despite the best efforts by the system owner to remove the malware or the presence of intruders on a network.

[77] Center, "APT1: Exposing One of China's Cyber Espionage Units," 27.

them. Delivery of the malware does not have to be done directly over the Internet as will be explored in the next example.

Buckshot Yankee

The cyber incident that led to Operation *Buckshot Yankee* was, as discussed in the introduction of this paper, a significant moment in the development of a true US Cyber capability in the centralized US Cyber Command. The malware called Agent.btz, which was discovered in October of 2008, achieved a foothold on the US DOD NIPRNET and SIPRNET.[78] This particular attack was significant in that, while it was not sophisticated malware, had been circulating on the Internet for months and was not causing any significant alarms until it was discovered on military networks, identifying that it was able to jump air gaps[79] without being detected.[80] Its precise origin is unknown, however it is likely that the malware was located on a USB memory stick that was found by a member of the US Army or a contractor at a base in the Middle East. This USB stick was inserted into a NIPRNET computer and spread throughout the network, infecting other USB memory sticks that were inserted into an infected machine. Eventually, one of these infected USB sticks was inserted in a classified computer connected to SIPRNET. The malware was designed to call back to a command and control server, possibly to download another piece of malware in order to establish persistence, or to extract information. This process of communicating to an external server is called beaconing.

---

[78] Nakashima, "Defense Official Discloses Cyberattack."

[79] Air gaps are physical separations between networks to attempt to isolate each network from each other to prevent the spreading of malware. This is generally done to separate networks were data of different classifications is to be stored/processed or to separate a corporate network from a development network.

[80] Karl Grindal, "Operation BUCKSHOT YANKEE," in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, ed. Jason Healey (Cyber Conflict Studies Association, 2013), 205.

It was this very beaconing to an Internet Protocol (IP) address that resided on the Internet that provided the first hint that the SIPRNET was infected, as a secret computer should not be attempting to contact an IP address on the Internet.[81] The beaconing was detected by a very keen analyst at the National Security Agency's (NSA) Advanced Networks Operation (ANO) team. The clean up operation that ensued was extremely costly, taking over 14 months to re-image all the affected computers.

As Ellen Nakashima, a national security reporter for The Washington Post, identifies in her article *Cyber-intruder sparks response, debate*, this incident was considered by officials at the Pentagon to be "the most serious breach" of DOD classified networks.[82] While no classified information was actually stolen from SIPRNET by Agent.btz, due to the air gap between SIPRNET and the Internet, the very fact that the malware achieved a foothold on the classified network demonstrates the potential for more sophisticated malware to jump back across to a network such as NIPRNET, which does have connections to the Internet, and could then extract the data slowly to its creator.

In response to the attack, the US DOD adopted draconian measures to prevent a similar infection from happening again. This involved banning the use of all removable media devices on DOD computers, such as USB memory sticks, CD/DVD disks, and flash media cards.[83] Eventually the rules were relaxed slightly to allow the use of DOD removable memory that had been scanned for viruses in order to permit essential transfer of information where no other means were possible, such as on the battlefield where limited bandwidth is available to transfer

---

[81] Ibid., 208.

[82] Ellen Nakashima, "Cyber-Intruder Sparks Response, Debate," *The Washington Post*, December 6, 2011, https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

[83] Grindal, "Operation BUCKSHOT YANKEE," 209.

large files.[84] However, this relaxation in regulations should be viewed with caution, as virus/malware scanners are limited in their ability to detect viruses without the correct signatures.[85] Specially crafted malware that has never been discovered before would bypass such a countermeasure against malware.

Such attacks on traditional IT networks illustrate the basics of hacking into a network and the usual target for the attacker, which is the data on a network, whether that be for intellectual property, the collection of intelligence data or military specifications for the latest military hardware. These techniques form the basis for attacking more complex systems, such as ICS.

Attacks on Industrial Control Systems

Stuxnet

Attacking industrial control systems requires a layered approach. Similar to attacks on traditional networks, attackers will attempt to discover vulnerabilities on a network during the reconnaissance phase. In ICS attacks however, this can be more difficult, as generally the control system network is usually kept physically separate from the corporate network, or is at least protected by firewalls, as discussed in Chapter 2. The reconnaissance phase is key in order to understand what control systems are in use. This allows attackers to find vulnerabilities to exploit in subsequent operations. The Stuxnet example from 2010 illustrates the vast amount of reconnaissance required to execute a complex cyber attack to achieve kinetic damage.

The malware called Stuxnet was revolutionary in its complexity, its ability to update itself and in the number of exploits it used in order to achieve its objective. Ralph Langner, a security researcher and owner of an independent cyber defence consultancy firm, compared Stuxnet to

---

[84] Ibid., 210.
[85] Skoudis and Liston, *Counter Hack Reloaded*, 581–82.

"an F-35 fighter jet on a World War I battlefield."[86] Stuxnet needed to attack three layers before achieving its objective of physically destroying the IR-1 nuclear refinement centrifuges.[87] The first layer was the IT layer, comprised of the traditional IT networks, operating systems and applications. The second layer was the ICS layer, which includes the industrial controllers and the supervisory applications. The third layer was the physical layer, such as valves, electrical motors, etc.

As Chris Morton, a public servant with influence on public policy at strategic levels of US government, recounts that Stuxnet was able to infiltrate the Natanz nuclear refinement facility's corporate network using four different Microsoft Windows zero-day[88] vulnerabilities, traversed to the engineering network by searching for Field Peripheral Gateways (PG), installed a malicious file in the PLC software development projects in the Siemens Step7 software to program PLCs on the engineering network, and then was installed on the PLCs themselves when engineers deployed the updated PLC software.[89] The malware was able to be installed on the latest Windows computers as it had loaded with valid authentication certificates that were stolen from Realtek, a well known vendor of audio cards for computers.[90] These certificates allowed the software to be installed without Windows raising any alarms to the operators, as it appeared that the software was a valid driver update.

The malware was able to replicate itself across networks and when it achieved persistence in the networks that contained the Field PGs, it would search for the PLCs that controlled the IR-

---

[86] Ralph Langner, "The Last Line of Cyber Defense," accessed April 17, 2016, http://www.langner.com/en/2010/11/19/the-big-picture/.

[87] Ralph Langner, "To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve" (The Langner Group, November 2013), 3–4, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

[88] Zero-day vulnerabilities are vulnerabilities in software that have not been discovered before and as such, no protection for these vulnerabilities exists until the first attack is discovered using the vulnerability.

[89] Morton, "Stuxnet, Flame, and Duqu - the OLYMPIC GAMES," in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, ed. Jason Healey (Cyber Conflict Studies Association, 2013), 221–22.

[90] Langner, "To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve," 11.

1 centrifuges. When these were found it would report back through its convoluted chain of air gaps to signal that it had reached its target to the command and control servers.[91] It would establish a "man-in-the-middle"[92] scenario whereby it would intercept all signals between the controller and the PLC, record the data and let through any commands while it was in its dormant state.[93] Once it received a command from the C2 server to activate the attack, it would replay the pre-recorded data to the controller, simulating a normal operating status of the PLC, while simultaneously feeding the PLC with malicious commands that led to the self-destruction of the centrifuges.[94]

The final indication of the level of sophistication of the Stuxnet worm is that it not only replicated itself, it was also able to update itself across all infected systems in order to continue its persistence within the networks should the system configurations change in order to combat Stuxnet.[95] In essence, the malware would attempt to spread itself to new machines, however if it detected that a version of itself was already present, it would verify its version and update it as required.

The very complexities of the Stuxnet worm and the fact that it targeted Iranian nuclear refinement centrifuges suggest that it was a state sponsored cyber attack. Although there has been no official declaration by the US that they were responsible for Stuxnet, David Sanger reported in the New York Times that senior officials from the US, Europe and Israel provided interviews supporting the narrative that Obama ordered the cyber attack on Iran's nuclear

---

[91] Morton, "Stuxnet, Flame, and Duqu - the OLYMPIC GAMES," 221.

[92] Man-in-the-middle is an attack whereby transmissions between computers or between processes on a computer are intercepted by a third computer or process in the middle of the communication path. This allows the attacker to intercept the communications as well as to modify the content of the communications to anything the attacker desires. The two computers or processes on either end are normally unaware that any break in the communications has occurred unless authentication for the traffic is used and is not compromised by the attacker.

[93] Langner, "To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve," 8–9.

[94] Ibid., 9.

[95] Morton, "Stuxnet, Flame, and Duqu - the OLYMPIC GAMES," 222.

enrichment facilities under an operation code named *Olympic Games*.[96] Given that the officials provided the interviews anonymously, the credibility of this story is unknown, despite the generally accepted view that the US and Israel were responsible for the attack. The complexity of the attack is definitely beyond the capabilities of typical cyber criminals, and the outcome is of the attack was strictly political.

Stuxnet opened the eyes of experts in the cyber domain to what is possible should a state decide to attack industrial control systems. This attack required a significant investment in time and money to craft various pieces of malware to first infiltrate the corporate networks, then to jump to the engineering networks and finally to the controllers in order to damage the machinery. This revealed the extent to which determined state actors will spend funding and resources in order to execute a cyber attack in order to achieve a strategic objective against another state. However, not all attacks against control systems need be this complicated to achieve physical damage. The next example will cover the attacks involving the damage to a blast furnace in a German steel mill.

German Steel Mill

In December of 2014, a report was released by the German Federal Office for Information Security, the Bundesamt für Sicherheit in der Informationstechnik (BSI), which discussed a cyber attack on a German steel mill plant.[97] While the report is only produced in German, several

[96] David E. Sanger, "Obama Ordered Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[97] Bundesamt für Sicherheitin der Infomationstechnik, "Die Lage Der IT-Sicherheit in Deutschland 2014," December 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile.

security news websites reported on the release of the report.[98] The cyber attack resulted in physical damage to a blast furnace in the plant. The BSI report provides few details about the attack itself, other than the fact that the attacker used spear-phishing techniques to access the corporate networks and that the attacker had knowledge of the ICS systems in the plant.[99]

The report was summarized in English by Robert Lee, Michael Assante and Tim Conway from the SANS institute's ICS division. Lee et al. note that the BSI report the incident as an APT attack but do not provide any details on their motive, which did not appear to be the common modus operandi of the APTs, namely, the theft of intellectual property.[100] The report also highlights the capabilities of the attackers. Given their ability to compromise the corporate networks through the use of spear phishing illustrates a proficiency in social engineering.[101] In addition, they displayed an in depth knowledge of the ICS they wished to attack, however the report does not provide any details on how the attacker jumped from the corporate network to the ICS network.[102]

While the report lacks details in order to fully analyze the attack on the German steel mill, likely to protect the identity of the mill and to prevent further attacks, it provides further evidence that attacks on ICS can lead to physical damage which, if used against a warship, could prevent it from sailing on its next mission. The next example will provide a third examination of an attack against an ICS where the result did not cause physical damage but lead to a power blackout for residents of the Ukraine.

---

[98] Eduard Kovacs, "Cyberattack on German Steel Plant Caused Significant Damage: Report | SecurityWeek.Com," accessed April 19, 2016, http://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report; Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *WIRED*, January 8, 2015, http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

[99] Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever."

[100] Robert M. Lee, Michael J. Assante, and Tim Conway, "German Steel Mill Cyber Attack," *Industrial Control Systems* 30 (2014): 3, http://ics3.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

[101] Ibid.

[102] Ibid.

Cyber Attack of a Ukrainian Power Grid

Thus far, the case studies illustrated in this section of this paper have been focused on illustrating the impact of cyber attacks on ICS resulting in physical damage to equipment within the facility under attack. However, attacks on ICS can result in damage outside of the facility, such as cutting power across multiple power grids. On 23 December 2015, 225,000 Ukrainian residents found themselves without electrical power for their homes as a result of a cyber attack.[103] Dustin Volz reporting for Reuters indicates that US cyber security researchers and cyber intelligence firms such as iSight Partners found evidence that a Russian hacking organization called "Sandworm" was responsible for the attack.[104]

This attack was highly coordinated and marks the first power grid to be taken offline as the result of a cyber attack.[105] Kim Zetter, a cyber security reporter for Wired Magazine, notes that operators at three power distribution centers observed their control computers mouse cursors move independently from their control and select and open circuit breakers at several substations, resulting in the loss of power to hundreds of thousands of residents.[106] Furthermore, the attackers were monitoring the operators actions, and prevented them from regaining control of their computers, logging them out of their session and changing their passwords.[107] According to Lee et al. the attackers also denied services to the power company's call center to prevent customers from reporting the loss of power.[108] Security experts were more impressed with the coordination of the operation than the malware used, as in the case of Stuxnet, the attackers spent

[103] Dustin Volz, "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage," *Reuters*, February 25, 2016, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K.

[104] Ibid.

[105] "Cyberattack That Crippled Ukrainian Power Grid Was Highly Coordinated - Technology & Science - CBC News," accessed April 20, 2016, http://www.cbc.ca/news/technology/ukraine-cyberattack-1.3398492.

[106] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *WIRED*, March 3, 2016, http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[107] Ibid.

[108] Robert M. Lee, Michael Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid" (Washington, D.C: Electricity Information Sharing and Analysis Center, March 18, 2016), 2.

months performing reconnaissance, obtaining credentials and ensuring the attack was well rehearsed.[109]

One of the important findings in the Lee report is that defenders need to focus on developing recovery procedures for "mission-critical" components in order to restore an affected system to operational status as soon as possible.[110] In the Ukrainian power grid attack, it took between one to six hours to restore the power to customers, however even months after the attack, the breakers were being operated manually as the firmware on the PLCs and had still not been remediated as of the 3rd of March, 2016.[111]

These three attacks on ICS illustrate the threats that exist towards warship control systems. All the equipment, from the computers running the supervisory control software to the PLCs controlling individual pieces of machinery used in civilian ICS such as in power plants and water purification facilities are identical in fit and function as those used in ships, with the only differences being in customization of the software and configuration of the equipment. While access to the ship systems should be more difficult due to security control measures surrounding military systems, it is not beyond the capabilities of determined foreign state actors, as was the case in the Natanz nuclear refinement facility. An additional concern that will be discussed in the next section of this chapter is the risk of embedded malware in counterfeit parts.

Attacks on the Supply Chain

Procurement of advanced military systems that constitute a warship involves a significantly complex supply chain. The various system components, while integrated by large

[109] Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid."
[110] Lee, Assante, and Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," 15.
[111] Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid."

defence contractors such as Lockheed Martin[112] or Northrop Grumman[113], come from different vendors, such as Siemens for PLCs, Saab and Thales for radars, etc, who may be sourcing some of their sub-components from other companies who obtained their parts from Asia. In fact, the BBC reported in May of 2012 that over 70% of approximately one million electronic components were found to be counterfeit parts and were traced back to China.[114] This information was reported by the Senate Armed Services Committee. The BBC identified that these counterfeit parts lead to an increase in risk posed to the operators of the military equipment. This elevated risk could be related to a reduced reliability of the counterfeit parts in comparison with the official parts.[115] However, what if these counterfeit parts were actually purposefully built and distributed to Western militaries in order to inject malware into their weapons systems or their ICS? The section will explore lower level types of malware that have been developed that could be used in counterfeit parts to undermine the reliability and integrity of military systems.

Firmware Hacks

What if you could infect a computer so thoroughly that even the most drastic of solutions to clean a computer, such as wiping the computer's hard drives clean and re-install the operating system, were unable to get rid of the malware? This type of malware would provide the attacker with complete control over the machine with the only possible fix being the replacement of the computer in its entirety. The software that first interacts with any computer or microcontroller is

---

[112] "HALIFAX Class Modernization · Lockheed Martin," accessed April 21, 2016, http://www.lockheedmartin.ca/ca/what-we-do/aerospace-defence/naval-systems/halifax-class-modernization.html.

[113] "Large Scale Systems Integration," *Northrop Grumman*, accessed April 21, 2016, http://www.northropgrumman.com/Capabilities/PublicSafety/Pages/LargeScaleSystemsIntegration.aspx.

[114] "China Fake Parts 'Used in US Military Equipment,'" *BBC News*, accessed April 21, 2016, http://www.bbc.com/news/world-us-canada-18155293.

[115] Ibid.

called firmware. The firmware is stored at the first memory location that the computer will read as soon as it is turned on and will initialize the devices on the computer, providing an interface between the hardware and the operating system. Malware can be written for microcontrollers or other low-level computing devices found within a computer that will intervene with the computer's normal operations before the operating system has a chance to load its files. When these malicious components are accessed by the operating system, they load malicious versions of files that are accessed by the operating system in order to interact with the devices. This gives hackers the ability to control the computer at the lowest level possible and maintain persistence even after the computer's administrator wipes the operating system and installs it anew.[116]

BadBIOS was reportedly the first malware found "in the wild" that overwrote the BIOS firmware on security researcher Dragos Ruiu's Macbook computer.[117] The Basic Input Output System (BIOS) is the memory space that contains the firmware for deskptop and laptop computers. It used to contain the drivers which allowed an operating system to interact with the hardware. While operating systems today contain drivers that allow interaction between the operating system and devices installed on the computer, the BIOS remains the first piece of code that a computer reads, allowing it to conduct hardware tests and boot the operating system.[118] Ruiu reported that the malware was able to transfer across computers using USB memory devices, that it was "operating system agnostic" (meaning that it would infect machines regardless of the operating system installed on the computer), and would prevent the computers

[116] Robert Graham, "Errata Security: #badBIOS Features Explained," accessed April 22, 2016, http://blog.erratasec.com/2013/10/badbios-features-explained.html.
[117] Vic Hargrave, "badBIOS – Sometimes 'Bad' is Really Bad -," March 21, 2014, http://blog.trendmicro.com/badbios-sometimes-bad-really-bad/.
[118] Graham, "Errata Security."

from booting off a CD-ROM.[119] It is believed that BadBIOS is the first BIOS level malware that is able to jump air gaps via USB memory sticks and using computers' speakers and microphones to transfer itself through ultrasonic communications.[120]

While there are certain experts such as Roger Grimes who are not convinced that Ruiu's discovery is credible,[121] there is sufficient evidence supporting Ruiu's individual claims about badBIOS that are covered by security expert Robert Graham, specifically the plausibility of infecting BIOS memory devices, transferring data over audio devices such as speakers and microphones,[122] and infecting USB devices.[123] Whether or not Ruiu actually had discovered malware capable of all of the above in one single package, the fact that these capabilities are possible at the firmware level is sufficiently troubling when considering supply chain risks.

Another example of firmware level malware that has been confirmed "in the wild" was discovered by security researcher Trammell Hudson. Thuderstrike is a firmware hack that exploits vulnerabilities in Apple's Extensible Firmware Interface (EFI) boot Read-Only Memory (ROM), a modern version of the BIOS. According to Husdson, Thunderstrike is able to write itself on the firmware of Apple's Thunderbolt devices[124] (such as hard drives) and once connected to an Apple computer, it can overwrite the EFI ROM in order to achieve persistence. Once it has taken over the computer, it is able to control the computer system, log keystrokes,

---

[119] Dragos Ruiu, "#badBIOS," *Google+*, accessed April 22, 2016, https://plus.google.com/app/basic/stream/z13tzhpzvpqyuzv1n23cz52wykrrvjjce.

[120] Dan Goodin, "Meet 'badBIOS,' the Mysterious Mac and PC Malware That Jumps Airgaps," *Ars Technica*, October 31, 2013, http://arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/.

[121] Roger A. Grimes, "Is BadBIOS Real?," *InfoWorld*, March 3, 2015, http://www.infoworld.com/article/2891692/security/does-the-latest-nsa-hack-prove-badbios-was-real.html.

[122] The transfer of data over audio was heavily used previously to transfer data over phone lines. Modems would transfer the data in audio format over the phone lines, which is why when modems connected to each other, the computer user could hear the squelching audio of the initial handshaking through the modem's speaker or on a telephone that was connected to the same line. This provided confirmation of the connection.

[123] Graham, "Errata Security."

[124] Thunderbolt is a proprietary hardware interface allowing the connection between external peripherals and computers designed by Apple and Intel. It is mainly used with Apple computers.

and spread through any Thunderbolt device.[125] A second vesion of the malware called Thunderstrike 2 was presented by Hudson, Xeno Kovah and Corey Kallenberg at the Black Hat conference in 2015. This version is able to spread via software over the Internet.[126] In both variants, the malware achieves persistence by exploiting the firmware that controls the booting sequence of the computer, before the operating system is loaded.[127] Again, this means that the computer cannot be sanitized by re-installing the operating system.

Both badBIOS and Thunderstrike provide evidence of existing malware that is able to exploit firmware vulnerabilities. Should a state embed malware with the capabilities described in either the badBIOS or Thunderstrike examples in counterfeit devices sold to Western militaries, they could raise significant doubts as to the trustworthiness of those military systems. The difficulty is actually detecting the malware should it be embedded in firmware in the first place. Dr. Aditya K Sood, a cyber-security expert and Dr. Richard Enbody, an Associate Professor in Computer Science and Engineering at Michigan State University identify that such counterfeit components were sold to the US military in 2011.[128] The Department of Homeland Security reported to the House Oversight and Government Reform Committee in July 2011 that many electronics sold to the US are preloaded with security compromising malware.[129] These findings undermine the trustworthiness of military systems until they can be confirmed to be free of

---

[125] Trammell Hudson, "Thunderstrike," *Trammell Hudson's Projects*, accessed April 24, 2016, https://trmm.net/Thunderstrike.

[126] Trammell Hudson, Xeno Kovah, and Corey Kallenberg, "Thunderstrike 2: Sith Strike - A MacBook Firmware Worm," accessed April 24, 2016, http://legbacore.com/Research_files/ts2-blackhat.pdf.

[127] Hudson, "Thunderstrike."

[128] Aditya K. Sood and Richard Enbody, "U.S. Military Defense Systems: The Anatomy of Cyber Espionage by Chinese Hackers | Georgetown Journal of International Affairs," accessed November 10, 2015, http://journal.georgetown.edu/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers/.

[129] Fahmida Rashid, "DHS Claims Foreign Suppliers Have Embedded Malware in U.S. Electronics," accessed April 24, 2016, http://www.eweek.com/c/a/Mobile-and-Wireless/DHS-Claims-Foreign-Suppliers-Have-Embedded-Malware-in-USElectronics-832422.

counterfeit components, if indeed this can truly be confirmed. This raises the importance of continuously monitoring the behaviour of systems to ensure that they are behaving as designed.

Conclusion

The exploits and cyber attacks presented in this chapter illustrate that military systems are just as vulnerable as typical corporate systems. The computers used on military corporate networks can be attacked using the same techniques as those employed against hospitals, educational institutions, corporations or government agencies. China actively targets defence contractors in order to obtain intellectual property on current and future military systems. [130] This information can give China an edge in not only developing their own advanced military systems, but also to create malware targeted specifically towards Western military systems.

Military systems that control weapons or mechanical control systems are susceptible to cyber attacks just like the control systems discussed in the Iranian nuclear refinement facility, the German steel mill and the Ukrainian power grid. While the latter two examples had networks that appeared to be directly connected to the Internet, the Natanz centrifuges were controlled on a network that was completely isolated from the Internet Connected corporate network. The fact that Stuxnet was able to jump air gaps, just like the Buckshot Yankee worm is sufficient evidence that military control systems could be attacked in a similar manner.

This chapter presented a brief historical overview of cyber attacks on systems that in one shape or another bear resemblance to the systems presented in Chapter 1. Given that

[130] Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies - The Washington Post," accessed November 9, 2015, https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

vulnerabilities in any information system or ICS will always be present, the RCN must be prepared to face cyber threats towards its ships.

CHAPTER 4

NAVAL CYBER OPERATORS

Introduction

Computer networks around the world are continuously under attack by black hat hackers. Daniel Ramsbrock, Robin Berthier and Michel Cukier, security researchers at the University of Maryland, conducted an experiment to quantify the behaviour of cyber attackers on vulnerable computers. In their IEEE conference paper *Profiling Attacker Behaviour Following SSH Compromises*, they noted an average of over 2,800 attacks per computer per day in their honeypot[131] over a period of 24 days.[132] This is equivalent to a computer being probed every 30 seconds.

While some computer systems on naval ships are connected to Defence networks via satellite communications and thus can connect to the Internet, these computers are being monitored by National Network Operations Centres (such as the Canadian Forces Network Operations Centre for the Canadian Armed Forces). However, computer systems used to control the machinery, the navigation and the combat systems of warships are generally kept completely separate, as in the *Halifax* class frigate, and thus are not susceptible to continuous scanning over the Internet. However, as was discussed in Chapter 2, there are ways for adversaries to jump those air gaps, be it through the use of USB memory sticks, by compromising defence contractor networks and embedding malware within system source code or by embedding malware in the firmware of counterfeit devices.

---

[131] Honeypots are computers or parts of a network that are designed and configured to attract cyber attackers so that their behaviours can be observed in a controlled and safe environment. In this study, the testbed contained four honeypot computers.

[132] Daniel Ramsbrock, Robin Berthier, and Michel Cukier, "Profiling Attacker Behavior Following SSH Compromises," in *Dependable Systems and Networks, 2007. DSN'07. 37th Annual IEEE/IFIP International Conference on* (IEEE, 2007), 119–124, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4272962.

As was mentioned in Chapter 1, good systems engineering will attempt to implement sound systems security engineering. However, as Tom Wolf, an expert in security engineering describes, no security program can guarantee perfect security, and a practical security solution is always determined with a view of coming at a reasonable cost to a given project.[133] In NIST 800-53, a heavy emphasis is placed on providing monitoring capabilities of the computer systems that comprise the entire system in the Audit and Accountability family of security controls, as well as in the Incident Response family.[134]

The Audit and Accountability family includes controls such as auditing events, audit review, analysis and reporting, audit reduction and report generation and non-repudiation. These controls outline how the organization will log, track and analyze security events on the system of interest.[135] In order to perform the auditing and analysis, certain tools, equipment and personnel training/education are required. The Incident Response family includes controls such as Incident Response training, incident handling, incident monitoring and incident reporting.[136] These controls determine how the organization handles an incident, how to contain the incident and how it recovers from the incident.

This chapter will discuss the equipment and personnel required in naval ICS, CMS and navigation systems in order to enable the navy to defend its networks and maintain the ship's capability to float, move and fight. It will first present the equipment required to be considered in the design of the systems to enable cyber defensive capabilities. It will then present the type of

---

[133] Tom W. Wolf, "A Brief Introduction to Security Engineering," *Tom W Wolf*, January 16, 2014, https://tomwwolf.com/2014/01/16/a-brief-introduction-to-security-engineering/.

[134] Joint Task Force Transformation Initiative, "NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations."

[135] Ibid., F-41-F-54.

[136] Ibid., F-103-F-111.

people required to defend the systems, the knowledge, education and training they need, and how they should fit into the ship's company.

Setting the Foundation for Cyber Defence – Required Equipment

Defence in depth is a well known concept in the information assurance (IA) security world. Bruce Schneier describes defence in depth as a means of enhancing security of a given IT system by overlapping varying security measures throughout the system layers.[137] Generally, these layers are established by using firewalls to segregate different sub-networks (called subnets) from each other. This, combined with the use of network Intrusion Detection Systems (IDS) and end-point[138] protection provides the defence-in-depth in order to protect a system from cyber attacks. Subnets that require external communications paths as well as internal are sandwiched between firewalls and are called DMZs. Galloway and Hancke describe this setup in their layered approach to a secured ICS, where the equipment requiring the ability to communicate between the corporate network and the industrial network is placed in the DMZ.[139]

In order to understand the layers in an IT system, a brief overview of the Open Systems Interconnection (OSI) model is required. The model contains seven layers that are used to describe the different communications functions in a computer network system. These layers are: the physical layer, the data link layer, the network layer, the transport layer, the session layer, the

[137] Bruce Schneier, "Security in the Cloud - Schneier on Security," accessed April 25, 2016, https://www.schneier.com/blog/archives/2006/02/security_in_the.html.

[138] End-points are generally considered to be the individual computers used by employees to conduct business, whether this be general business such as email and word processing or the operation of SCADA systems from the supervisor console.

[139] Galloway and Hancke, "Introduction to Industrial Control Networks," 876.

presentation layer and the application layer.[140] The layers of most importance in this paper are the transport, session and application layers, however the others will be quickly explained.

The physical layer describes the physical components that allow for the physical transmission of the data. It includes the network cables, radio transceivers, modems, fibre optic cables, network interface controllers (NIC) and transmission schemes, such as voltage levels to differentiate between 1's and 0's.[141]

The data link layer defines a means to provide error-free data transfer by separating data streams into frames and arranging for the sequencing of the frames while transferring them over the physical layer.[142] An example of a data link protocol is the Address Resolution Protocol, which allows NICs to tell the gateways that their media access control address (their physical address) is related to which IP address. It is this protocol which is normally attacked in traditional man-in-the-middle attacks.[143]

The network layer is concerned with the routing of the data frames between the origin and destination of the information. Devices operating at this layer determine the best routing for the transmission of the data.[144] A well known protocol is the Internet protocol (IP) which provides the addressing scheme over IP networks.

The transport layer defines how messages are transferred sequentially and without errors, duplications or losses between hosts.[145] While there are many transport protocols, the two most common in network traffic are the Transmission Control Protocol (TCP) and the User Datagram Protocol. TCP is generally used for longer, more complex and session-based communications,

---

[140] "The OSI Model's Seven Layers Defined and Functions Explained," accessed April 25, 2016, https://support.microsoft.com/en-us/kb/103884.
[141] Ibid.
[142] Ibid.
[143] Skoudis and Liston, *Counter Hack Reloaded*, 482.
[144] "The OSI Model's Seven Layers Defined and Functions Explained."
[145] Ibid.

while UDP is used for simple messaging, such as lookups of Uniform Resource Locator (URL) addresses or for synchronizing time on a network.[146]

The session layer provides single session communications between two different devices.[147] This is done by using ports that are listened to by services such as a web or email server. A user attempting to establish communications with these servers will send a synchronization request to the ports that these services are listening to. Many popular services listen to standardized ports, such as port 80 for web pages, port 443 for encrypted web pages, port 25 or 587 for email, etc.[148] This layer is often used by hackers to determine what services are offered on any given device. This attack is called port scanning. An attacker will attempt to find vulnerable services that they can exploit.[149]

The presentation layer prepares the information for the applications on the devices. It provides the encoding/decoding protocols for the conversion of bytes to character codes as well as data compression/decompression and encryption/decryption.[150]

Finally, the application layer allows users and applications on a device to communicate with the network. It is this layer that interprets the data that is transferred over the network and presents it to the user in the application, such as the web browser or the email client.[151]

Firewalls are devices that monitor the connections into and out of networks or end-point devices and decide whether the communications should be allowed to pass through.[152] A firewall usually operates at the network, transport and session layers as it is able to filter communications based on IP address, transport protocol used or ports. They allow system administrators to

---

[146] Skoudis and Liston, *Counter Hack Reloaded*, 33–43.
[147] "The OSI Model's Seven Layers Defined and Functions Explained."
[148] Skoudis and Liston, *Counter Hack Reloaded*, 268.
[149] Ibid.
[150] "The OSI Model's Seven Layers Defined and Functions Explained."
[151] Ibid.
[152] Skoudis and Liston, *Counter Hack Reloaded*, 56.

control which IP addresses and ports within a network can communicate externally as well as which communications are allowed into the network. For example, if an external computer is requesting communications with a company's web server on port 80, a firewall would allow the communication into the web server. The web server would be in the DMZ of the network, so should an external computer attempt to connect to an end-user computer using port 80, the firewall would block this communication.

While firewalls provide some security based on IP addresses and port numbers, typical attacks following an initial compromise of a system on a network establish a command and control channel via a port that is usually left open, such as port 80 to allow workers access to Internet pages. In order to detect these command and control channels, deep packet inspection is required.

An IDS and its sister device, the Intrusion Prevention System (IPS), is a device that monitors network communications and looks for malicious behaviour.[153] Similar to anti-virus or anti-malware software, an IDS can use signature based detection and anomaly based detection in order to determine if traffic on a network is behaving maliciously.[154] A signature based IDS will compare network traffic with known malicious behaviour, such as contacting known malicious IP addresses or URLs, emails being transferred with title names and file attachments with suspicious names such as "Free pictures" and "freepics.exe."[155] An anomaly based detection will compare known behaviour of the typical traffic on a network with any events that occur and attempt to find traffic that is considerably different from the normal behaviour on the network.[156]

---

[153] Karen Scarfone and Peter Mell, "NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)," *NIST Special Publication* 800, no. 2007 (2007): 2–1.

[154] Skoudis and Liston, *Counter Hack Reloaded*, 65.

[155] Scarfone and Mell, "NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)," 2–4.

[156] Ibid.

IDS and IPS can be network based and host[157] based. Either solution provides significant logging and alerting capabilities that allow network administrators to analyse events in order to determine if their network has been breached. The host based type of IDS is a form of end-point protection.

End-point protection or end-point security solutions are software packages that are deployed to the computers on a network where there is typically user interaction, such as desktop computers in an office environment. Endpoint security can be viewed as the evolutionary product of anti-virus software. As described by Rick Moy, endpoint security solutions are software products that are deployed on the networked computers and include a multitude of security features, such as malware quarantining, anti-spyware, end-point firewall, a built in IDS, application permissions as well as control of data flow in and out of the computer.[158] Just as the IDS devices at the network level can detect malicious behaviour using signatures or anomaly based detection schemes, so too do end-point security solutions for malware detection. The problem with both signature and anomaly based detection is that both IDS and end-point security solutions are prone to identifying false positives and false negatives, that is, identifying events falsely as malicious or missing malicious events altogether.[159] These false identifications need to be reviewed by skilled technicians to determine the validity of the detections and their impact on the network.

There are many more security devices that can increase security in a network. However, firewalls, IDS/IPS and end-point protection form the base required to effectively manage a

---

[157] A host is any computer connected to a network that is usually interacted with by a user.

[158] Michael Kassner, "Endpoint Security: What Makes It Different from Antivirus Solutions," *TechRepublic*, accessed April 29, 2016, http://www.techrepublic.com/blog/it-security/endpoint-security-what-makes-it-different-from-antivirus-solutions/.

[159] Chris Sanders and Jason Smith, *Applied Network Security Monitoring: Collection, Detection and Analysis* (Elsevier, 2013), 159.

network, detect malicious activity and respond. These devices need to be configured with correct network settings and up-to-date signatures, their logs and alerts must be reviewed in order to determine if breaches occur, and when breaches do occur, an appropriate response must be taken to ensure that mission critical tasks can still be performed on the network. Thus there is a requirement for personnel trained and educated in network security in order.

Human in the Loop – Personnel, Training and Education

Assuming a network has been properly designed with all the correct security controls, tools and devices put in place, there remains a requirement to have dedicated personnel responsible for maintaining the security posture of the network. This entails reviewing the configurations of the devices on the network to ensure they have not changed from the approved baseline, that logs and events are reviewed in order determine if malicious behaviour has occurred on the network, to neutralize malicious behaviour while maintaining as much of the network functionality as possible and returning the system to a known good state after an attack has been discovered and neutralized.[160] This is known as "continuous monitoring". In addition, the signatures required to detect malicious traffic or malware on and end-point must be kept updated and the anomaly based detection devices must be kept tuned to changes in the legitimate behaviour of the network. For this to happen, ships will require personnel onboard to conduct the activities above.

The US Navy has recognized the requirement for the defence of networks at sea. Admiral Jonathan Greenert, Chief of Naval Operations for the US Navy discussed the navy's requirement to seize the initiative in the future battle domain of EM and cyber in his US Naval Institute

[160] Eugene Schultz, "Continuous Monitoring: What It Is, Why It Is Needed, and How to Use It" (SANS Institute, June 2011), 3, https://www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-is-needed-35030.

Proceedings conference paper *Imminent Domain.* His view is that by making EM-cyber operations a fully integrated element of naval operations alongside the traditional land, sea, air and space domains, rather than alongside them, the USN can stay ahead of adversaries who will try to exploit the same capabilities.[161] While Greenert focuses his discussion on the broader EM-cyber operations, Vice Admiral (Retired) Nancy Brown, Captain Danelle Barrett and Lieutenant-Commander Jesse Castillo, US Navy specialists in information technology, argue that naval cyber warfare officers and enlisted sailors are needed and must be deployed with ships at sea in order to defend the multitude of networks as presented in Chapter 1.[162]

In order to ensure that the right people are employed to perform the task of continuous monitoring, the RCN must understand that these people must think like hackers and must know the networks on the ship better than anyone else. In a presentation at the USENIX Enigma 2016 conference, the Chief of Tailored Access Operations of the NSA Rob Joyce stated that in order to defend a network, the defenders need to understand that network and the devices connected to it better than the original designers, because nation state hackers will collect information on their target such that they know it better than its designers and administrators.[163]

Hackers are ingenious people who like to explore, tinker, disassemble and make things perform beyond their expectations.[164] In order to defend networks from malicious hackers, the defenders must think like the attackers, and thus be hackers themselves. Lieutenant-Colonel Gregory Conti, a Military Intelligence Officer and Director of West Point's Cyber Security Research Center and Lieutenant-Colonel David Raymond, and Armour Officer and Assistant

---

[161] Jonathan W. Greenert, "Imminent Domain," *United States Naval Institute Proceedings* 138(12) (December 2012): 16–21.

[162] Nancy Brown, Danelle Barrett, and Jesse Castillo, "CREATING Cyber Warriors.," *U.S. Naval Institute Proceedings* 138, no. 10 (October 2012): 28–32.

[163] Rob Joyce, "Disrupting Nation State Hackers" (USENIX Enigma 2016, San Francisco, California, January 28, 2016), https://www.youtube.com/watch?v=bDJb8WOJYdA.

[164] Levy, *Hackers: Heroes of the Computer Revolution - 25th Anniversary Edition*, 20.

Professor in West Point's Department of Electrical Engineering and Computer Science identified this need in their article, *Leadership of Cyber Warriors*. They highlight the need for cyber warriors to have very strong technical capabilities, be able to solve complex problems creatively and be hackers.[165] They note that, while a typical soldier may own their own firearms at home, a cyber warrior is more likely to have his own malware analysis laboratory at home.[166] However, they also discuss the leadership challenges involved with leading a group of hackers in a military environment, as they are typically non-conformist and respect technical prowess and problem solving skills rather than management skills.[167] Thus cyber leaders must also have a hacker mentality.

This is not significantly different from how engineering departments in the RCN are structured. The leader of the combat systems engineering department is usually a computer or electrical engineer who understands the technical capabilities and the scientific theory behind how the combat systems function, while the technicians are the technical experts who maintain the equipment. The engineering officer provides a link between the operational commander of the ship, the Captain, and is able to translate the technical language related to the status of the equipment to the operational impact that the Commanding Officer (CO) needs to know.

Thus, should the RCN build a cyber defence capability onboard ships, it will need both cyber defender operators and cyber defense officers who are at least as technically proficient in general cyber capabilities so that the cyber defenders will respect and trust its leadership. The cyber defense officer would provide the operational impact of cyber events to the Captain and lead his team to mitigate the attacks while maintaining the warship's capabilities in accordance

[165] Gregory Conti and David Rayond, "Leadership of Cyber Warriors: Enduring Principles and New Directions," *Small Wars Journal*, July 2011, 3.
[166] Ibid., 4.
[167] Ibid.

with the warfare priority as determined by the CO. This construct is similar to how the combat systems engineering department functions when the ship is under Action Stations.[168]

The RCN's Emergency Response Team (ERT) Manual describes how the RCN organizes its departments for various warfighting or emergency situations in order to maintain the ship's ability to float, move and fight, specifically with respect to how the combat systems engineering department supports the battle by maintaining the combat systems operational during an engagement.[169] The department is broken down into repair teams and is dispatched to spaces that have taken damage or where systems are experiencing faults and attempt to rectify the systems in order to maintain the ship's fighting capability. The Combat Systems Engineering Officer is responsible for advising command on impacts to the operational state of the ship and for recommending courses of action to meet the command's warfighting priority.

A cyber defense team onboard the ship should have a similar structure of cyber operators monitoring all the networks and an officer reporting to command on the status of the networks and advising command on events. When a response is required which may impact the ship's ability to float, move and fight, the cyber officer would advise command on the impact to the command priority before ordering his team to take action. This requires that the officer and cyber defenders understand how a ship fights, how the systems onboard support all of the ship's functions and how they impact the varying command priorities.

One approach to creating cyber operators for the RCN would be to create a pan Canadian Armed Forces (CAF) occupation and deploying small teams to ships that are themselves deploying to operational theatres. This would leverage the general education and training

[168] Action Stations is the state where ship's personnel are at their assigned stations for warfighting and systems are ready to combat in accordance with the assigned priority: anti-air warfare, anti-surface warfare, anti-sub surface warfare, etc.

[169] Department of National Defence, "B-GN-007-RCN/FP-002, CFCD 133 Royal Canadian Navy Emergency Response Team Manual" (Canada, July 1, 2015).

funding for such an occupation and increase the pool of candidates. However, this would limit the team's ability to understand how a warship functions and, more critically, would not allow the cyber defenders to truly understand the ship's systems as well as if they were navy specific cyber defenders with additional training of the ship's systems. If Rob Joyce's statement regarding the required knowledge to defend a network holds true, and given the differences of the naval systems described in Chapter 1, it is unreasonable to expect any cyber operator to be temporarily affected to a naval ship and effectively defend that network. Another approach would be to have dedicated naval cyber operators employed in a shore based facility with a remote data link into the ship's networks. While this approach would allow for more room onboard the ships for other occupations to fill the limited bunk space, it is unrealistic to expect that the data link will always be available. Deploying the cyber operators onboard ship allows them to always be able to monitor the networks, especially during critical evolutions such as engagements with the enemy or even replenishments at sea, and to be completely cognisant of the command priority at all times during these evolutions.

Training and education requirements for naval cyber operators will certainly have commonality with general cyber operators for the CAF. Many cyber operators joining the CAF may already have education at the Bachelor or Masters level.[170] However, for those without this level of education, the RCN must ensure that they know how to think critically and evaluate situations effectively in a cyber contested environment. In the vernacular, training and education are often used interchangeably. For the purposes of this paper, training is defined as repetitive exercise used to analyse situations and respond accordingly to solve a problem, similar to how pilots are trained to respond to in-flight emergencies. Education is defined as the act of learning

[170] Conti and Rayond, "Leadership of Cyber Warriors: Enduring Principles and New Directions," 4.

how to think and analyse problems without any pre-defined solutions. Or rather, as Lauren Resnick, an educational psychologist at the University of Pittsburgh defines in *Education and Learning to Think*, higher order thinking is complex, solutions are not fully specified in advance, can lead to several solutions and requires "nuanced judgement".[171] Thus, training cyber operators on the systems will be insufficient because training will limit them to only knowing how to take action, but not how to think and to resolve problems that have never been seen before.

Education early on in the career of a cyber operator will be essential to developing their critical thinking abilities that will be needed to analyse network activities in the most stressing of circumstances at sea. Navy and system specific education and training should follow in order to prepare cyber operators to perform at sea under pressure. Finally, a significant amount of "red team"[172] exercises on a recurring basis will provide the necessary reinforcement of the skills and abilities of the cyber operators while also challenging them to continually learn in order to combat new hacking techniques and tools. Colonel Robert Turk of the US Army acknowledges this in *Preparing a Cyber Security Workforce for the 21st Century*, where he argues that "complementing training with realistic cyber-exercises will prove invaluable to readiness as well as fully operationalize cyber into the warfighting domains."[173]

Although the advances in technology have vastly improved many aspects of naval operations, the threat to this new technology through the exploitation of its vulnerabilities presents an opportunity for the navy to return to some of its roots. The combat capabilities and the mechanical systems require the computation power of the systems currently being fitted in

---

[171] L.B. Resnick and S.T.E. Committee on Research in Mathematics, *Education and Learning to Think* (National Academies Press, 1987), 3, https://books.google.ca/books?id=_zYrAAAAYAAJ.

[172] Red team exercises are activities where an adversary is provided by a friendly organization to simulate a real world adversary attempting to penetrate the friendly network.

[173] Robert W. Turk, "Preparing a Cyber Security Workforce for the 21st Century" (United States Army War College, March 2013), 11, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA561195.

modern warships, but non-technological solutions can still work for navigation. The USN has already taken steps to re-train its navigators in the use of sextants and paper charts in order to be able to navigate their ships following the loss of their navigation systems or access to GPS.[174] The RCN should also re-introduce traditional navigation techniques to its navigators as well as seek other opportunities where possible to become less reliant on technology in order to function.

Conclusion

Naval cyber operators will be required to defend the RCN's warships from cyber attacks. History has shown us that when hackers have the right will, they can penetrate any network desired, such as the examples provided in Chapter 2. No system can be made impenetrable. Therefore, when designing systems that will be networked on warships, the engineers must ensure that they consider the right tools that need to be incorporated into the system to permit cyber operators to monitor the system and respond to events.

The right tools include perimeter defenses, such as firewalls that control the flow in and out of the networks, IDS/IPS devices that inspect the network traffic for malicious behaviour and end-point protection that observes the behaviour of specific devices on the network. These devices must be maintained in order to ensure that the networks are functioning accordingly and are delivering the mission capabilities required of the ship and its command. This includes updating their configurations to allow for updates to the network, to adjust for equipment failures, or to isolate cyber attacks.

The people required to operate these monitoring tools must be able to think like the attackers in order to defeat them. They must be hackers themselves. They need to be able to

[174] Geoff Brumfiel, "U.S. Navy Brings Back Navigation By The Stars For Officers," *NPR.org*, accessed May 2, 2016, http://www.npr.org/2016/02/22/467210492/u-s-navy-brings-back-navigation-by-the-stars-for-officers.

think critically and learn on their own in order to stay current with the latest attack techniques. This means they need to be educated in order to ensure that they have the higher-order thinking abilities to combat cyber attackers. They also need to be trained specifically on naval systems in order to know their networks better than those who designed them and must truly understand how they support the ship's mission. This means that the job could not be assigned temporarily to general cyber operators who had not been trained on the navy and warship systems.

Naval cyber operators will need to be continually exercised to ensure that they truly know their systems and can respond appropriately to intrusions on their networks and keep the ships floating, moving and fighting.

Finally, the RCN should seek to increase training in areas of seamanship that can serve as a backup to the technology found in the ships, such as in areas of navigation where the reliance on GPS and INS can be supported by an ability to navigate by the stars using old tools such as sextants.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

This paper set out to explore the general vulnerabilities of the computer networks on modern warships in order to highlight the importance of creating naval cyber operators to defend these systems. The modern warship is highly reliant on computer networks to function in the modern age and be able to counter existing air, surface and subsurface threats. These networks operate systems that control the mechanical equipment required to ensure the ship can float and move, the navigation equipment that ensures the ship can be safely navigated and the combat systems required so that the ship can be used to exercise deadly force or to protect itself or other vessels in its care from threats. As explained in Chapter 2, there are three categories of systems to consider on warships when looking at cyber threats to ship systems: ICS, navigation systems and CMS.

The level of complexity of a modern warship's machinery requires an ICS to effectively manage and operate it. As this computer network is responsible for controlling the propulsion machinery, the electrical power distribution and the ancillary systems such as ballast pumps and damage control equipment, the network itself is a critical component to the survivability of the ship.

The navigation systems provide an essential capability for the safety of a ship at sea. Accurate ship positioning on electronic charts in real-time with radar overlay of land masses and other shipping in the area is a key requirement to safe navigation, especially in limited visibility situations. In order to deliver such a capability, a navigation system is made up of many sub-systems that are required, such as GPS, navigation radars, ECDIS, INS and a navigation data distribution. All of these systems require computers to run their unique software applications.

Modern CMS allow warships to detect, localize, classify and prosecute the various threats such as anti-ship missiles, fighter bombers, submarines and torpedoes. The CMS provides a C2 picture via inputs from the tracking radars, the ESM system and the sonar systems and controls the weapons and ECM systems, allowing operators to prosecute the threats to the ship, as well as build the recognized maritime picture for a given area. Just as the ICS and navigation systems, CMSs are comprised of computer networks with customized software.

The majority of these systems use COTS software and hardware in many of the components. COTS contain the same vulnerabilities as the systems deployed in civilian networks. For example, The Windows operating system is the same on a ECDIS that it is on a computer sold in any electronics store, provided that it is the same version of Windows and is patched to the same level (e.g. Windows XP versus Windows 7). The computer systems onboard ships also have MOTS, unique software applications and unique hardware that may only be found in these types of systems. However, this does not guarantee that they are free from any vulnerabilities that could be exploited.

The examples presented in Chapter 3 illustrate attacks on traditional networks for the purposes of cyber espionage, as well as attacks on critical infrastructure and ICS such as the Stuxnet malware used to attack the Iranian nuclear refinement facility at Natanz, the German steel mill plant and the Ukrainian power grid. In all of these examples, traditional networks were used as stepping stones to the control systems by jumping air gaps. Finally, Chapter 3 also presented the threats to military systems by introducing malware in counterfeit components at the firmware level. These examples demonstrate that military systems are vulnerable to the same types of attacks as can happen in the civilian sector should nation state actors decide to exploit vulnerabilities in military systems.

Given that naval systems have similar vulnerabilities to other computer networks that could be exploited in similar fashions as the examples of Chapter 3, it behooves the RCN to prepare itself for cyber attacks against its systems. With proper systems engineering processes that incorporate systems security engineering, as discussed in Chapter 2, including the consideration for monitoring tools in the systems that were discussed in Chapter 4, the RCN requires naval cyber operators to monitor the ICS, navigation and CMS systems for malicious network traffic and anomalous behaviour. These cyber defenders must be hackers themselves, able to think like their adversaries in order to detect malicious activities on the critical systems. They must be given the opportunities to be educated in hacking first principles in order to think with agility and quickly learn the complexities of new systems. They must know their systems better than the designers. Most importantly they must understand naval operations to ensure that they provide the ship's command team with the requisite availability of the systems dependant on the battle priority should a cyber attack occur in the middle of a conventional naval engagement.

In order to achieve this capability, the RCN needs to develop a naval cyber operator occupation. This occupation will require knowledge in traditional enterprise networking, combat systems and industrial control systems. It is likely that the initial cadre of naval cyber operators will come from three streams: current Naval Weapons Engineering technicians, Marine Systems Engineering technicians, Naval Electricians and Naval Communicators. These four occupations currently have some training in the operations of the combat and navigation systems, the ICS and the enterprise networks respectively, however this training is limited to general administration of the networks or simply preventive and corrective maintenance of the equipment. Similarly, naval cyber officers should initially be sought out from the existing pools of Combat Systems

Engineering Officers, Marine Systems Engineering Officers and Maritime Surface and Subsurface Officers with an Information Management Director qualification. None of these occupations have any cyber education or training. Nonetheless, it is likely that within these occupations there may be some individuals who already possess a hacker mentality or have skills in networking that would lend them to be excellent candidates to become cyber operators. The RCN should seek out these individuals in order to develop the naval cyber operator occupation. The initial education could be achieved through sponsored post-graduate training in cyber security or equivalent at the college level. This would be followed up by practical exercising with shipboard simulators.

The RCN will also need to target recruiting efforts towards civilian hackers who may be attracted to working in an exciting field and who would enjoy the naval lifestyle. Not many civilian hackers would have the opportunity to interact with the diversity of systems found on warships. These civilians would enter the military just as with any other occupation and receive specific training on the shipboard systems to complement their existing knowledge of cyber security.

Finally, the RCN will have to integrate the naval cyber operators into ships' companies. It is recommended that they be integrated into the Combat Systems Engineering Department as the cyber section and have an officer at the director level placed in charge of the team, reporting to the Combat Systems Engineering Officer but with a direct line to command during naval engagements. Further study should be conducted to assess other ways to integrate the cyber operators into a ship's company.

As the number of cyber events continues to grow every year and the results of these events have increasing consequences, it is imperative that the RCN develop a capability to

monitor, respond, isolate and recover from cyber attacks to its ships. This can only be done with navy specific cyber operators who can link the impacts of degradations to the shipboard networks to naval capabilities.

BIBLIOGRAPHY

"About ECDIS | What Is ECDIS? | | ECDIS." Accessed April 7, 2016. http://www.ecdis-info.com/about_ecdis.html.

Balduzzi, Marco. "AIS Exposed - Understanding Vulnerabilities & Attacks 2.0." presented at the Black Hat Asia, March 2014. https://www.blackhat.com/docs/asia-14/materials/Balduzzi/Asia-14-Balduzzi-AIS-Exposed-Understanding-Vulnerabilities-And-Attacks.pdf.

Bensing, Richard G. "An Assessment of Vulnerabilities for Ship-Based Control Systems." Monterey, California. Naval Postgraduate School, 2009. http://calhoun.nps.edu/handle/10945/4646.

"Bromium Endpoint Protection & Endpoint Security." Accessed April 11, 2016. https://www.bromium.com/.

Brown, Nancy, Danelle Barrett, and Jesse Castillo. "CREATING Cyber Warriors." *U.S. Naval Institute Proceedings* 138, no. 10 (October 2012): 28–32.

Brumfiel, Geoff. "U.S. Navy Brings Back Navigation By The Stars For Officers." *NPR.org*. Accessed May 2, 2016. http://www.npr.org/2016/02/22/467210492/u-s-navy-brings-back-navigation-by-the-stars-for-officers.

Bundesamt für Sicherheitin der Infomationstechnik. "Die Lage Der IT-Sicherheit in Deutschland 2014," December 2014. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile.

Center, Mandiant Intelligence. "APT1: Exposing One of China's Cyber Espionage Units." Mandiant, 2013.

"China Fake Parts 'Used in US Military Equipment.'" *BBC News*. Accessed April 21, 2016. http://www.bbc.com/news/world-us-canada-18155293.

Conti, Gregory, and David Rayond. "Leadership of Cyber Warriors: Enduring Principles and New Directions." *Small Wars Journal*, July 2011, 10.

Copeland, B. Jack. *Colossus: The Secrets of Bletchley Park's Code-Breaking Computers*. OUP Oxford, 2006.

Crawford, George. "New Roles for Information Systems in Military Operations." *Air & Space Power Chronicles*. Accessed April 11, 2016. http://www.iwar.org.uk/iwar/resources/airchronicles/crawford.htm.

"Cyberattack on German Steel Plant Caused Significant Damage: Report | SecurityWeek.Com." Accessed April 6, 2016. http://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report.

"Cyberattack That Crippled Ukrainian Power Grid Was Highly Coordinated - Technology & Science - CBC News." Accessed April 20, 2016. http://www.cbc.ca/news/technology/ukraine-cyberattack-1.3398492.

Department of National Defence. "B-GN-007-RCN/FP-002, CFCD 133 Royal Canadian Navy Emergency Response Team Manual." Canada, July 1, 2015.

"Endpoint Security | Detect and Block Endpoint Attacks." *FireEye*. Accessed April 11, 2016. https://www.fireeye.com/products/hx-endpoint-security-products.html.

Furr, Steve. "What Is Real Time and Why Do I Need It?" *Military Embedded Systems Resource Guide*, 2002. http://pdf.cloud.opensystemsmedia.com/mil-embedded.com/QNX.May05.pdf.

Gallagher, Sean. "The Navy's Newest Warship Is Powered by Linux." *Ars Technica*, October 18, 2013. http://arstechnica.com/information-technology/2013/10/the-navys-newest-warship-is-powered-by-linux/.

Galloway, B., and G. P. Hancke. "Introduction to Industrial Control Networks." *IEEE Communications Surveys Tutorials* 15, no. 2 (Second 2013): 860–80. doi:10.1109/SURV.2012.071812.00124.

Geer, David. "Security of Critical Control Systems Sparks Concern." *Computer* 39, no. 1 (January 2006): 20–23. doi:10.1109/MC.2006.32.

GICSP, Ernie Hayden, Michael Assante, and Tim Conway. "An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity," 2014. https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf.

Goodin, Dan. "Meet 'badBIOS,' the Mysterious Mac and PC Malware That Jumps Airgaps." *Ars Technica*, October 31, 2013. http://arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/.

Gorman, Siobhan. "Electricity Grid in U.S. Penetrated By Spies." *Wall Street Journal*, April 9, 2009, sec. Tech. http://www.wsj.com/articles/SB123914805204099085.

Gorman, Siobhan, August Cole, and Yochi Dreazen. "Computer Spies Breach Fighter-Jet Project." *Wall Street Journal*, April 21, 2009, sec. Tech. http://www.wsj.com/articles/SB124027491029837401.

Graham, Robert. "Errata Security: #badBIOS Features Explained." Accessed April 22, 2016. http://blog.erratasec.com/2013/10/badbios-features-explained.html.

Greenert, Jonathan W. "Imminent Domain." *United States Naval Institute Proceedings* 138(12) (December 2012): 16–21.

Grimes, Roger A. “Is BadBIOS Real?” *InfoWorld*, March 3, 2015. http://www.infoworld.com/article/2891692/security/does-the-latest-nsa-hack-prove-badbios-was-real.html.

Grindal, Karl. “Operation BUCKSHOT YANKEE.” In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, edited by Jason Healey, 205–11. Cyber Conflict Studies Association, 2013.

“Hackers Hit 100 Banks in ‘Unprecedented’ $1 Billion Cyber Heist: Kaspersky Lab | SecurityWeek.Com.” Accessed April 4, 2016. http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab.

“HALIFAX Class Modernization · Lockheed Martin.” Accessed April 21, 2016. http://www.lockheedmartin.ca/ca/what-we-do/aerospace-defence/naval-systems/halifax-class-modernization.html.

Hargrave, Vic. “badBIOS – Sometimes ‘Bad’ is Really Bad -,” March 21, 2014. http://blog.trendmicro.com/badbios-sometimes-bad-really-bad/.

“Harpoon Block II Anti-Ship Missile.” *Naval Technology*. Accessed April 11, 2016. http://www.naval-technology.com/projects/harpoon-block-ii-anti-ship-missile/.

Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association, 2013.

Heckman, Kristin E., Frank J. Stech, Ben S. Schmoker, and Roshan K. Thomas. “Denial and Deception in Cyber Defense.” *Computer* 48, no. 4 (2015): 36–44.

Hudson, Trammell. “Schedule 31. Chaos Communication Congress.” Accessed April 24, 2016. https://events.ccc.de/congress/2014/Fahrplan/events/6128.html.

———. “Thunderstrike.” *Trammell Hudson’s Projects*. Accessed April 24, 2016. https://trmm.net/Thunderstrike.

Hudson, Trammell, Xeno Kovah, and Corey Kallenberg. “Thunderstrike 2: Sith Strike - A MacBook Firmware Worm.” Accessed April 24, 2016. http://legbacore.com/Research_files/ts2-blackhat.pdf.

International Maritime Organization (IMO). “International Convention for the Safety of Life at Sea,” November 1, 1974.

Joint Task Force Transformation Initiative. “NIST Special Publication 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems.” National Institute of Standards and Technology, June 2014. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.

———. “NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations.” National Institute of Standards and

Technology, April 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Joint Task Force Transformation Initiative, and others. “NIST Special Publication 800-39: Managing Information Security Risk.” National Institute of Standards and Technology, March 2011. http://dl.acm.org/citation.cfm?id=2206266.

Joyce, Rob. “Disrupting Nation State Hackers.” presented at the USENIX Enigma 2016, San Francisco, California, January 28, 2016. https://www.youtube.com/watch?v=bDJb8WOJYdA.

Kantharia, Raunek. “What Is Integrated Bridge System (IBS) on Ships?” *Marine Insight*, April 16, 2012. http://www.marineinsight.com/marine-navigation/what-is-integrated-bridge-system-ibs-on-ships/.

Kassner, Michael. “Endpoint Security: What Makes It Different from Antivirus Solutions.” *TechRepublic*. Accessed April 29, 2016. http://www.techrepublic.com/blog/it-security/endpoint-security-what-makes-it-different-from-antivirus-solutions/.

King, A. D. “Inertial Navigation-Forty Years of Evolution.” *GEC Review* 13, no. 3 (1998): 140–149.

Kovacs, Eduard. “Cyberattack on German Steel Plant Caused Significant Damage: Report | SecurityWeek.Com.” Accessed April 19, 2016. http://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report.

Langner, Ralph. “The Last Line of Cyber Defense.” Accessed April 17, 2016. http://www.langner.com/en/2010/11/19/the-big-picture/.

———. “To Kill a Centrifuge - A Technical Analysis of What Stuxnet’s Creators Tried to Achieve.” The Langner Group, November 2013. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

“Large Scale Systems Integration.” *Northrop Grumman*. Accessed April 21, 2016. http://www.northropgrumman.com/Capabilities/PublicSafety/Pages/LargeScaleSystemsIntegration.aspx.

Lee, Robert M., Michael Assante, and Tim Conway. “Analysis of the Cyber Attack on the Ukrainian Power Grid.” Washington, D.C: Electricity Information Sharing and Analysis Center, March 18, 2016.

Lee, Robert M., Michael J. Assante, and Tim Conway. “German Steel Mill Cyber Attack.” *Industrial Control Systems* 30 (2014). http://ics3.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

Levy, Steven. *Hackers: Heroes of the Computer Revolution - 25th Anniversary Edition*. O’Reilly Media, 2010. https://books.google.ca/books?id=mShXzzKtpmEC.

Meinel, Carolyn. “Computer Hacking: Where Did It Begin and How Did It Grow?” *WindowSecurity.com*, October 16, 2002. http://www.windowsecurity.com/whitepapers/harmless_hacking_book/Computer_hacking_Where_did_it_begin_and_how_did_it_grow_.html.

Merkow, M.S., and J. Breithaupt. *Information Security: Principles and Practices*. Certification/Training Series. Pearson Education, 2014. https://books.google.ca/books?id=YBKpAwAAQBAJ.

Minsky, Amy. “‘Anonymous’ Claims Responsibility for Cyber Attack That Shut down Government Websites | Globalnews.ca,” June 17, 2015. http://globalnews.ca/news/2060036/government-of-canada-servers-suffer-cyber-attack/.

Mitchell, Bradley. “What Is Hacking?” *About.com Tech*, February 26, 2016. http://compnetworking.about.com/od/networksecurityprivacy/f/what-is-hacking.htm.

Morton. “Stuxnet, Flame, and Duqu - the OLYMPIC GAMES.” In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, edited by Jason Healey. Cyber Conflict Studies Association, 2013.

Nakashima, Ellen. “Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies - The Washington Post.” Accessed November 9, 2015. https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

———. “Cyber-Intruder Sparks Response, Debate.” *The Washington Post*, December 6, 2011. https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

———. “Defense Official Discloses Cyberattack.” *The Washington Post*, August 25, 2010, sec. Politics. http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html.

“Navigation Integrated Bridge System – Marine Systems - L-3 MAPPS.” Accessed April 6, 2016. http://www.mapps.l-3com.com/navigation-integrated-Bridge-System.html.

“Network Security Products and Solutions.” *Cisco*. Accessed April 11, 2016. http://www.cisco.com/c/en/us/products/security/index.html.

“New Sonar Developments.” *Naval Technology*, February 28, 2011. http://www.naval-technology.com/features/feature111462/.

Peyvandi, Hossein, Mehdi Farrokhrooz, Hossein Roufarshbaf, and Sung-Joon Park. “SONAR Systems and Underwater Signal Processing: Classic and Modern Approaches.” In *Sonar Systems*, edited by Nikolai Kolev. InTech, 2011.

http://www.intechopen.com/books/sonar-systems/sonar-systems-and-underwater-signal-processing-classic-and-modern-approaches.

Ramsbrock, Daniel, Robin Berthier, and Michel Cukier. “Profiling Attacker Behavior Following SSH Compromises.” In *Dependable Systems and Networks, 2007. DSN’07. 37th Annual IEEE/IFIP International Conference on*, 119–124. IEEE, 2007. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4272962.

Rashid, Fahmida. “DHS Claims Foreign Suppliers Have Embedded Malware in U.S. Electronics.” Accessed April 24, 2016. http://www.eweek.com/c/a/Mobile-and-Wireless/DHS-Claims-Foreign-Suppliers-Have-Embedded-Malware-in-USElectronics-832422.

Reed, John. “Did Chinese Espionage Lead To F-35 Delays? |.” Accessed April 14, 2016. http://www.defensetech.org/2012/02/06/did-chinese-espionage-lead-to-f-35-delays/.

Resnick, L.B., and S.T.E. Committee on Research in Mathematics. *Education and Learning to Think*. National Academies Press, 1987. https://books.google.ca/books?id=_zYrAAAAYAAJ.

Ruiu, Dragos. “#badBIOS.” *Google+*. Accessed April 22, 2016. https://plus.google.com/app/basic/stream/z13tzhpzvpqyuzv1n23cz52wykrrvjjce.

Sanders, Chris, and Jason Smith. *Applied Network Security Monitoring: Collection, Detection and Analysis*. Elsevier, 2013.

Sanger, David E. “Obama Ordered Wave of Cyberattacks Against Iran.” *The New York Times*, June 1, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

Scarfone, Karen, and Peter Mell. “NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS).” *NIST Special Publication* 800, no. 2007 (2007): 94.

Schneier, Bruce. “Security in the Cloud - Schneier on Security.” Accessed April 25, 2016. https://www.schneier.com/blog/archives/2006/02/security_in_the.html.

Schultz, Eugene. “Continuous Monitoring: What It Is, Why It Is Needed, and How to Use It.” SANS Institute, June 2011. https://www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-is-needed-35030.

Skolnik, Merrill. *Introduction to Radar Systems*. Third. McGraw-Hill Professional, 2001.

———. *Radar Handbook, Third Edition*. 3rd ed. McGraw-Hill Professional, 2008.

Skoudis, Edward, and Tom Liston. *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. 2nd ed. Prentice Hall, 2006.

Sood, Aditya K., and Richard Enbody. “U.S. Military Defense Systems: The Anatomy of Cyber Espionage by Chinese Hackers | Georgetown Journal of International Affairs.” Accessed November 10, 2015. http://journal.georgetown.edu/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers/.

Stoll, Clifford. “Cuckoo’s Egg: Stalking the Wily Hacker.” In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, edited by Jason Healey, 89–106. Cyber Conflict Studies Association, 2013.

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. “NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security.” National Institute of Standards and Technology, June 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

“The OSI Model’s Seven Layers Defined and Functions Explained.” Accessed April 25, 2016. https://support.microsoft.com/en-us/kb/103884.

Turk, Robert W. “Preparing a Cyber Security Workforce for the 21st Century.” United States Army War College, March 2013. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA561195.

UK Hydrographic Office. “ECDIS Buyers Guide,” September 2012. http://www.gnsworldwide.com/sites/default/files/ecdis_buyers_guide_v2_0_19_09_12.pdf.

Volz, Dustin. “U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage.” *Reuters*, February 25, 2016. http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K.

Wolf, Tom W. “A Brief Introduction to Security Engineering.” *Tom W Wolf*, January 16, 2014. https://tomwwolf.com/2014/01/16/a-brief-introduction-to-security-engineering/.

Zetter, Kim. “A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever.” *WIRED*, January 8, 2015. http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

———. “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon | WIRED.” Accessed November 6, 2015. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

———. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.” *WIRED*, March 3, 2016. http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.